ONLINE SAFETY BILL

EXPLANATORY NOTES

What these notes do

These Explanatory Notes relate to the Online Safety Bill as brought from the House of Commons on 18 January 2023 (HL Bill 87).

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

Table of Contents

Subject **Page of these Notes**

Overview of the Bill 7

Policy background 7

Existing Regulation of Online Services 7
The Online Harms White Paper 8
Interim Codes of Practice 10
Government Report on Transparency Reporting 10
Pre-legislative Scrutiny 10
The Online Safety Bill 11

Legal background 14

Territorial extent and application 16

Commentary on provisions of Bill 17

Part 1: Introduction 17
- Clause 1: Overview of Act 17

Part 2: Key definitions 17
- Clause 2: "User-to-user service" and "search service" 17
- Clause 3: "Regulated service", "Part 3 service" etc 18
- Clause 4: Disapplication of Act to certain parts of services 20

Part 3: Providers of regulated user-to-user services and regulated search services: Duties of care 21

Chapter 1: Introduction 21
- Clause 5: Overview of Part 3 21

Chapter 2: Providers of user-to-user services: duties of care 21
- Clause 6: Providers of user-to-user services: duties of care 21
- Clause 7: Scope of duties of care 21
- Clause 8: Illegal content risk assessment duties 21
- Clause 9: Safety duties about illegal content 22
- Clause 10: Children's risk assessment duties 24
- Clause 11: Safety duties protecting children 24
- Clause 12: User empowerment duties 26
- Clause 13: Duties to protect content of democratic importance 27
- Clause 14: Duties to protect news publisher content 27
- Clause 15: Duties to protect journalistic content 28
- Clause 16: Duty about content reporting 29
- Clause 17: Duties about complaints procedures 29
- Clause 18: Duties about freedom of expression and privacy 30
- Clause 19: Record-keeping and review duties 31

Chapter 3: Providers of search services: duties of care 31
- Clause 20: Providers of search services: duties of care 31

These Explanatory Notes relate to the Online Safety Bill as brought from the House of Commons on 18 January 2023 (HL Bill 87).

Clause 21: Scope of duties of care 32
Clause 22: Illegal content risk assessment duties 32
Clause 23: Safety duties about illegal content 33
Search services likely to be accessed by children 33
Clause 24: Children's risk assessment duties 33
Clause 25: Safety duties protecting children 34
Clause 26: Duty about content reporting 35
Clause 27: Duties about complaints procedures 35
Clause 28: Duties about freedom of expression and privacy 35
Clause 29: Record-keeping and review duties 36
Chapter 4: Children's Access Assessments 36
Clause 30: Children's access assessments 36
Clause 31: Duties about children's access assessments 37
Clause 32: Meaning of "likely to be accessed by children" 37
Chapter 5: Duties about fraudulent advertising 37
Clause 33: Duties about fraudulent advertising: Category 1 services 37
Clause 34: Duties about fraudulent advertising: Category 2A services 38
Clause 35: Fraud etc offences 39
Chapter 6: Codes of practice and guidance 39
Clause 36: Codes of practice about duties 39
Clause 37: Codes of practice: principles, objectives, content 39
Clause 38: Procedure for issuing codes of practice 41
Clause 39: Secretary of State's powers of direction 41
Clause 40: Procedure for issuing codes of practice following direction under section 39 42
Clause 41: Publication of codes of practice 43
Clause 42: Review of codes of practice 43
Clause 43: Minor amendments of codes of practice 43
Clause 44: Relationship between duties and codes of practice 43
Clause 45: Effects of codes of practice 44
Clause 46: Duties and the first codes of practice 44
Clause 47: OFCOM's guidance about certain duties in Part 3 44
Clause 48: OFCOM's guidance: content that is harmful to children and user empowerment 45
Chapter 7: Interpretation of Part 3 45
Clause 49: "Regulated user-generated content", "user-generated content", "news publisher content" 45
Clause 50: "Recognised news publisher" 46
Clause 51: "Search content", "search results" etc 46
Clause 52: Restricting users' access to content 47
Clause 53: "Illegal content" etc 47
Clause 54: "Content that is harmful to children" etc 50
Clause 55: Regulations under section 54 50
Clause 56: Regulations under section 54: OFCOM's review and report 51
Part 4: Other duties of providers of regulated user-to-user services and regulated search services 51
Chapter 1: User identity verification 51
Clause 57: User identity verification 51
Clause 58: OFCOM's guidance about user identity verification 51
Chapter 2: Reporting Child Sexual Exploitation and Abuse Content 51
Clause 59: Requirement to report CSEA content to the NCA 51
Clause 60: Regulations about reports to the NCA 52
Clause 61: NCA: information sharing 53
Clause 62: Offence in relation to CSEA reporting 53
Clause 63: Interpretation of this Chapter 53
Chapter 3: Terms of service: Transparency, accountability, and freedom of expression 54
Clause 64: Duty not to act against users except in accordance with terms of service 54
Clause 65: Further duties about terms of service 54
Clause 66: OFCOM's guidance about duties set out in sections 64 and 65 55

Clause 67: Interpretation of this Chapter 55
Chapter 4: Transparency Reporting 56
Clause 68: Transparency reports about certain Part 3 Services 56
Clause 69: OFCOM's guidance about transparency reports 56
Part 5: Duties of providers of regulated services: Certain pornographic content 57
Clause 70: "Pornographic content", "provider pornographic content" "regulated provider pornographic content" 57
Clause 71: Scope of duties about regulated provider pornographic content 57
Clause 72: Duties about regulated provider pornographic content 59
Clause 73: OFCOM's guidance about duties set out in section 72 59
Part 6: Duties of providers of regulated services: fees 59
Clause 74: Duty to notify OFCOM 59
Clause 75: Duty to pay fees 60
Clause 76: OFCOM's statement about "qualifying worldwide revenue" etc 60
Clause 77: Threshold figure 60
Clause 78: Secretary of State's guidance about fees 60
Clause 79: OFCOM's fees statements 61
Clause 80: Recovery of OFCOM's initial costs 61
Clause 81: Meaning of "charging year" and "initial charging year" 62
Part 7: OFCOM's powers and duties in relation to regulated services 62
Chapter 1: General Duties 62
Clause 82: General duties of OFCOM under section 3 of the Communications Act 62
Clause 83: Duties in relation to strategic priorities 62
Clause 84: Duty to carry out impact assessments 63
Chapter 2: Register of categories of regulated user-to-user services and regulated search services 63
Clause 85: Meaning of threshold conditions etc 63
Clause 86: Register of categories of certain Part 3 services 65
Clause 87: Duty to maintain register 65
Clause 88: List of emerging Category 1 services 66
Chapter 3: Risk assessments of regulated user-to-user services and regulated search services 66
Clause 89: OFCOM's register of risks, and risk profiles, of Part 3 services 66
Clause 90: OFCOM's guidance about risk assessments 67
Chapter 4: Information 67
Clause 91: Power to require information 67
Clause 92: Information notices 67
Clause 93: Requirement to name a senior manager 67
Clause 94: Reports by skilled persons 68
Clause 95: Investigations 68
Clause 96: Power to require interviews 68
Clause 97: Powers of entry, inspection and audit 69
Clause 98: Offences in connection with information notices 70
Clause 99: Senior managers' liability: information offences 71
Clause 100: Offences in connection with notices under Schedule 12 71
Clause 101: Other information offences 71
Clause 102: Penalties for information offences 71
Clause 103: Co-operation and disclosure of information: overseas regulators 71
Clause 104: Disclosure of information 72
Clause 105: Intelligence service information 72
Clause 106: Provision of information to the Secretary of State 73
Clause 107: Amendment of Enterprise Act 2002 73
Clause 108: Information for users of regulated services 74
Clause 109: Admissibility of statements 74
Chapter 5: Regulated user-to-user services and regulated search services: notices to deal with terrorism content and CSEA content 74

Clause 110: Notices to deal with terrorism content or CSEA content (or both) 74
Clause 111: Warning notices 75
Clause 112: Matters relevant to a decision to give a notice under section 110(1) 75
Clause 113: Notices under section 110(1): supplementary 75
Clause 114: Review and further notice under section 110(1) 76
Clause 115: OFCOM's guidance about functions under this Chapter 76
Clause 116: OFCOM's annual report 77
Clause 117: Interpretation of the Chapter 77
Chapter 6: Enforcement Powers 77
Clause 118: Provisional notice of contravention 77
Clause 119: Requirements enforceable by OFCOM against providers of regulated services 77
Clause 120: Confirmation decisions 78
Clause 121: Confirmation decisions: requirements to take steps 78
Clause 122: Confirmation decisions: risk assessments 78
Clause 123: Confirmation decisions: children's access assessments 78
Clause 124: Confirmation decisions: proactive technology 79
Clause 125: Confirmation decisions: penalties 79
Clause 126: Penalty for failure to comply with confirmation decision 80
Clause 127: Penalty for failure to comply with notice under section 110(1) 80
Clause 128: Non-payment of fee 80
Clause 129: Information to be included in notices under sections 127 and 128 80
Clause 130: Amount of penalties etc 80
Clause 131: Service restriction orders 82
Clause 132: Interim service restriction orders 82
Clause 133: Access restriction orders 82
Clause 134: Interim access restriction orders 83
Clause 135: Interaction with other action by OFCOM 83
Clause 136: Publication by OFCOM of details of enforcement action 83
Clause 137: Publication by providers of details of enforcement action 83
Clause 138: OFCOM's guidance about enforcement action 84
Chapter 7: Committees, research and reports 84
Clause 139: Advisory committee on disinformation and misinformation 84
Clause 140: Functions of the Content Board 84
Clause 141: Research about users' experiences of regulated services 84
Clause 142: Consumer consultation 84
Clause 143: OFCOM's statement about freedom of expression and privacy 85
Clause 144: OFCOM's reports about news publisher content and journalistic content 85
Clause 145: OFCOM's transparency reports 85
Clause 146: OFCOM's report about researchers' access to information 85
Clause 147: OFCOM's reports 85
Part 8: Appeals and super-complaints 86
Chapter 1: Appeals 86
Clause 148: Appeals against OFCOM decisions relating to the register under section 86 86
Clause 149: Appeals against OFCOM notices 86
Chapter 2: Super-complaints 86
Clause 150: Power to make super-complaints 86
Clause 151: Procedure for super-complaints 87
Clause 152: OFCOM's guidance about super-complaints 87
Part 9: Secretary of State's functions in relation to regulated services 87
Clause 153: Statement of strategic priorities 87
Clause 154: Consultation and parliamentary procedure 88
Clause 155: Directions about advisory committees 88
Clause 156: Directions in special circumstances 88
Clause 157: Secretary of State's guidance 89
Clause 158: Annual report on the Secretary of State's functions 89

These Explanatory Notes relate to the Online Safety Bill as brought from the House of Commons on 18 January 2023 (HL Bill 87).

Clause 159: Review 89
Part 10: Communications offences 90
Clause 160: False communications offence: England and Wales 90
Clause 161: Exemptions from offence under section 160 90
Clause 162: Threatening communications offence: England and Wales 90
Clause 163: Interpretations of sections 160 to 162 91
Clause 164: Offences of sending or showing flashing images electronically: England and Wales and Northern Ireland 91
Clause 165: Extra-territorial application and jurisdiction 93
Clause 166: Liability of corporate officers 93
Clause 167: Sending etc photograph or film of genitals 93
Clause 168: Repeals in connection with offences under sections 160 and 162 94
Clause 169: Consequential amendments 94
Part 11: Supplementary and General 96
Clause 170: Providers' judgements about the status of content 96
Clause 171: OFCOM's guidance about illegal content judgements 96
Clause 172: Providers that are not legal persons 97
Clause 173: Individuals providing regulated services: liability 97
Clause 174: Liability of parent entities etc 97
Clause 175: Former providers of regulated services 97
Clause 176: Information offences: supplementary 98
Clause 177: Defences 98
Clause 178: Liability of corporate officers for offences 98
Clause 179: Application of offences to providers that are not legal persons 98
Clause 180: Extra-territorial application 99
Clause 181: Information offences: extra-territorial application and jurisdiction 99
Clause 182: Payment of sums into the Consolidated Fund 99
Clause 184: Service of notices 99
Clause 185: Amendments of Part 4B of the Communications Act 100
Schedule 16: Amendments of Part 4B of the Communications Act 100
Clause 186: Repeal of Part 4B of the Communications Act 100
Clause 187: Repeal of Part 4B of the Communications Act: transitional provision etc 100
Schedule 17: Video sharing platform services: transitional provision etc 100
Clause 188: Repeals: Digital Economy Act 2017 101
Clause 189: Offence under the Obscene Publications Act 1959: OFCOM defence 101
Clause 190: Offences regarding indecent photographs of children: OFCOM defence 102
Clause 191: Powers to amend section 35 102
Clause 192: Powers to amend or repeal provisions relating to exempt content or services 102
Clause 193: Powers to amend Part 2 of Schedule 1 103
Clause 194: Powers to amend Schedules 5, 6 and 7 103
Clause 195: Power to make consequential provision 103
Clause 196: Regulations: general 103
Clause 197: Parliamentary procedure for regulations 104
Part 12: Interpretation and final provisions 104
Clause 198: "Provider" of internet service 104
Clause 199: "User", "United Kingdom user" and "interested person" 105
Clause 200: "Internet service" 105
Clause 201: "Search engine" 105
Clause 202: "Proactive technology" 106
Clause 203: Content communicated "publicly" or "privately" 107
Clause 204: "Functionality" 107
Clause 205: "Harm" etc 107
Clause 206: "Online safety functions" and "online safety matters" 107
Clause 207: Interpretation: general 107
Clause 208: Index of defined terms 107
Clause 209: Financial provisions 107

Clause 210: Extent 108
Clause 211: Commencement and transitional provision 108
Clause 212: Short title 108

Commencement 109

Financial implications of the Bill 109

Parliamentary approval for financial costs or for charges imposed 109

Compatibility with the European Convention on Human Rights 110

Compatibility with the Environment Act 2021 110

Related documents 110

Annex A – Territorial extent and application in the United Kingdom 112

Subject matter and legislative competence of devolved legislatures 117

Overview of the Bill

1 The Online Safety Bill establishes a new regulatory regime to address illegal and harmful content online. It imposes legal requirements on:

- Providers of internet services which allow users to encounter content generated, uploaded or shared by other users ("user-to-user services");
- Providers of of search engines which enable users to search multiple websites and databases ("search services"); and
- Providers of internet services on which provider pornographic content (pornographic content that is published by a provider and is not user-generated) is published or displayed.

2 The Bill confers new powers on the Office of Communications (OFCOM) enabling them to act as the online safety regulator. This role will include overseeing and enforcing the new regulatory regime.

Policy background

3 As use of the internet has expanded, there is growing public concern about the prevalence and spread of illegal online content, as well as the risks to children's safety arising from exposure to inappropriate content, such as pornography.

4 Recent research and public polling has also highlighted users' concerns about how platforms are applying their own terms and conditions, and how they respond to users' complaints.

Existing Regulation of Online Services

5 At present, most user-to-user and search services operating in the United Kingdom are not subject to any regulation concerning user safety.

6 A limited number of user-to-user services which are used in the United Kingdom are subject to the Video Sharing Platform regime set out in Part 4B of the Communications Act 2003 (the "VSP Regime"). Only services which meet the legal definition of a video sharing platform[1] and has the required connection with the United Kingdom[2] are in scope.

7 Services subject to the VSP Regime are required to take measures to:

a. Protect the public from videos and adverts likely to incite violence or hatred against a person on specified grounds including sex, race, colour, ethnic or social origin, genetic

[1] The legal test is set out in Section 368S of the Communications Act 2003. OFCOM have produced guidance on the definition of a video sharing platform which is available on the OFCOM website.

[2] Sections 368S(3)-(5) of the Communications Act 2003 sets out when a video sharing platform will be regarded as having the required connection with the United Kingdom for the purposes of the VSP Regime. OFCOM have produced guidance in relation to when a video sharing platform will be regarded as established in the United Kingdom, which is available on the OFCOM website.

features, language, religion or belief, political opinion, membership of a national minority, disability, age and sexual orientation;

b. Protect the public from material in videos or adverts where the inclusion of that material would be a criminal offence under laws relating to terrorism, child sexual abuse material, and racism and xenophobia;

c. Protect under 18s from videos and adverts which have or would be likely to be given an R18 certificate,[3] or which have been or would likely be refused a certificate by the British Board of Film Classification;[4] and

d. Protect under 18s from videos and adverts containing material that might impair their physical, mental or moral development.

8 The VSP Regime does not set standards for the content of individual videos.

9 OFCOM are responsible for enforcing video sharing platform providers' compliance with their obligations under the VSP Regime. OFCOM have the power to give enforcement notifications (which may set out the steps required to remedy a contravention)[5] and to impose financial penalties of up to £250,000 or 5% of qualifying revenue, whichever is greater.[6] In certain circumstances, OFCOM may also suspend and/or restrict a service.[7]

The Online Harms White Paper

10 The Online Harms White Paper, published in April 2019, set out the Government's intention to introduce a new regulatory framework to improve protections for users online. It was proposed that this objective would be achieved via a new duty of care on companies, and an independent regulator responsible for overseeing the online safety framework. The White Paper proposed that the regulatory framework should follow a proportionate and risk-based approach, and that the duty of care should be designed to ensure that all in-scope companies had appropriate systems and processes in place to address harmful content and improve the safety of their users.

11 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.

---

[3] The R18 category is a special and legally-restricted classification, primarily for explicit videos of consenting sex or strong fetish material involving adults, and where the primary purpose of the material is sexual arousal or stimulation.

[4] The BBFC's current guidelines outline that material likely to be unsuitable for classification could include: material which is in breach of criminal law (or created through the commission of a criminal offence); material that appears to risk harm to individuals or to society such as, for example, the detailed portrayal of violence or dangerous acts, illegal drug use; and the portrayal or invitations to conduct sadistic violence, rape or other non-consensual sexual violent behaviour or other harmful violent activities.

[5] Sections 368Z2 and 368Z3 of the Communications Act 2003.

[6] Section 368Z4 of the Communications Act 2003.

[7] Sections 368Z5 and 368Z6 of the Communications Act 2003.

12 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 but harmful 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.

13 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 United Kingdom, 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 their regulatory functions and funding.

d. Part 4 explained the proposed functions of the regulator, including their 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

14 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 online harms regulator issues codes of practice using the powers conferred by the Bill.

Government Report on Transparency Reporting

15 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.

Pre-legislative Scrutiny

16 In May 2021 the Online Safety Bill was published in draft. A Joint Committee of MPs and Peers, chaired by Damian Collins MP, was established on 23 July 2021 to carry out pre-legislative scrutiny. The Joint Committee took evidence from over 50 witnesses and received over 200 pieces of written evidence. The Committee published its report and recommendations on 10 December 2021.

17 The Government responded to the report on 17 March 2022 confirming that a number of substantive changes were made to the Bill at introduction, including, but not limited to:

a. Including priority offences in primary, rather than secondary legislation;

b. Including a new standalone provision for non-user-generated pornography, meaning all providers of online pornography will be within scope of the legislation;

c. Including the Law Commission's recommendations for new online communications offences;

d. Amending the senior manager liability offence so that it is no longer deferred, and will instead be commenced three months after Royal Assent;

e. Including a new duty on Category 1[8] providers to offer optional user verification and user empowerment tools on their sites;

f. Including a new duty on Category 1 and Category 2A providers to protect users from fraudulent advertising online; and

g. Simplifying the definition of non-designated harmful content, and requiring Category 1 providers only to address categories of content that are legal but harmful to adults, which are designated in secondary legislation.

[8] Category 1 services will be a subset of user-to-user services that will have additional duties placed on them.

The Online Safety Bill

18 The new legislation will impose legal requirements on:

a. Providers of internet services which allow users to encounter content generated, uploaded or shared by other users, i.e. user-generated content ("user-to-user services");

b. Providers of search engines which enable users to search multiple websites and databases ("search services"); and

c. Providers of internet services on which provider pornographic content is published or displayed.

19 The legislation will require providers of regulated user-to-user and search services to:

a. Assess their user base and the risks of harm to those users present on the service;

b. Take steps to mitigate and manage the risks of harm to individuals arising from illegal content and activity, and (for services likely to be accessed by children) content and activity that is harmful to children. Changes were made in the House of Commons to the illegal content duties meaning that companies will now need to assess the risk of their services being used for the commission or facilitation of a priority offence and to design and operate their services to mitigate this risk;

c. Put in place systems and processes which allow users and affected persons to report specified types of content and activity to the service provider;

d. Establish a transparent and easy to use complaints procedure which allows for complaints of specified types to be made;

e. Have particular regard to the importance of protecting users' legal rights to freedom of expression and protecting users from a breach of a legal right to privacy when implementing safety policies and procedures; and

f. Put in place systems and processes designed to ensure that detected but unreported CSEA content is reported to the NCA.

20 Those user-to-user services which meet the Category 1 threshold conditions, specified by the Secretary of State, will be subject to additional legal requirements, including to:

a. Improve transparency and accountability and protect free speech. These duties follow changes made in the House of Commons to remove the previous adult safety duties from the Bill ("legal but harmful"). Those user-to-user services which meet the Category 1 threshold conditions must have systems and processes to ensure they only remove or restrict access to content, or ban or suspend users, except where allowed by their terms of service, or where they otherwise have a legal obligation to do so.

a. Carry out an assessment of the impact that safety policies and procedures will have on users' legal rights to freedom of expression, including on access to and treatment

of news publisher and journalistic content, and users' privacy, and demonstrate the steps they have taken to mitigate any impact;

b. Specify in a public statement the steps taken to protect users' legal rights to freedom of expression and users' privacy;

c. Put in place systems and processes designed to ensure that the importance of the free expression of content of democratic importance is taken into account when making decisions about how to treat such content;

d. Put in place systems and processes designed to ensure that the importance of the free expression of journalistic content is taken into account when making decisions about how to treat such content.

e. Notify and offer a right of appeal to a recognised news publisher before removing or moderating its content, or taking action against its account, following changes made in the House of Commons;

f. Put in place a dedicated and expedited complaints procedure that ensures that the decisions of the service provider to take action against a user because of a particular piece of journalistic content can be challenged;

g. Offer optional user verification and user empowerment tools to adults on their sites; and

h. Put in place proportionate systems and processes to prevent the risk of users encountering fraudulent adverts.

21 Those search services which meet the Category 2A threshold conditions will be under a duty to produce annual transparency reports and to put in place proportionate systems and processes to prevent the risk of users encountering fraudulent adverts.

22 The Bill confers new powers on OFCOM enabling them to act as the online safety regulator. OFCOM will be responsible for enforcing the legal requirements imposed on service providers. The Bill gives OFCOM the power to compel in-scope providers to provide information and to require an individual from an in-scope provider to attend an interview; powers of entry and inspection; and the power to require a service provider to undertake, and pay for, a report from a skilled person.

23 The new powers conferred on OFCOM also include the power to give enforcement notifications (which may set out the steps required to remedy a contravention) and the power to impose financial penalties of up to £18 million or 10% of qualifying worldwide revenue, whichever is greater. If a service provider fails to comply with a confirmation decision, OFCOM can, in certain circumstances, apply to the Courts for an order imposing business disruption measures on that provider.

24 The Bill requires OFCOM to produce codes of practice for service providers, setting out the recommended steps that providers can take in order to comply with the legal requirements

described above. A provider may take different measures to those recommended in the codes of practice. A provider will be treated as having complied with the relevant legal obligation if the provider takes the steps recommended in the relevant code of practice for complying with that obligation.

25 The Bill also requires providers of internet services which make pornographic material available by way of the service (as opposed to enabling users to generate or share such content) to ensure that children are not normally able to encounter that pornographic content.

26 The Bill creates a new false communications offence and a new threatening communications offence and amends the existing communications offences in the Malicious Communications Act 1988 and Section 127 of the Communications Act 2003 to reflect this. It also creates a new "cyberflashing" offence and specific offences of sending or showing flashing images electronically to people with epilepsy intending to cause them harm.

Legal background

27 Prior to the United Kingdom'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)[9]. 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.

28 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.

29 The status of the eCD following the United Kingdom'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 United Kingdom to legislate in line with the provisions of the eCD following the end of the transition period on 31 December 2020.

30 The Audiovisual Media Services Regulations 2020 transposed the EU's revised Audiovisual Media Services Directive (AVMSD)[10] into United Kingdom law. The AVMSD introduced a new regulatory framework for video sharing platforms. A principal feature of a video sharing platform is that it enables users to upload and share videos with members of the public (with the platform having no editorial control over the content of the video). The Government transposed the VSP framework into Part 4B of the Communications Act 2003, which came into force on 1 November 2021. Further detail on the current regulation of video sharing platforms is set out above.

31 Other related legislation includes the Digital Economy Act 2017 ("DEA"). Section 103 of the DEA obliges the Secretary of State to issue a code of practice for providers of online social media platforms setting out guidance on action it might be appropriate for social media providers to take to prevent bullying, insulting, intimidating and humiliating behaviours on their sites. The code of practice was published on 8 April 2019. Part 3 of the DEA 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

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

[10] 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.

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.

32 OFCOM are the independent regulator for communications in the United Kingdom. Their remit covers the regulation of broadband and telecoms, TV, radio, video-on-demand services and postal services. They are also responsible for managing the effective use of the radio spectrum.

33 OFCOM were established under the Office of Communications Act 2002. OFCOM are a statutory corporation, and their governance arrangements are set out in the Office of Communications Act 2002. As a public authority, OFCOM are also subject to other legal duties, including requirements to ensure they act in a way that is compatible with human rights (under the Human Rights Act 1998) and comply with data protection legislation.

34 OFCOM's powers are found in the Communications Act 2003 and the Wireless Telegraphy Act 2006, as well as other enactments including the Broadcasting Acts 1990 and 1996, and the Postal Services Act 2011. 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.

35 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), Part 4 of the Audiovisual Media Services Regulations 2020 (S.I. 2020/1062) (which inserts Part 4B into the Communications Act 2003), and Regulation 4 of the Audiovisual Media Services (Amendment) (EU Exit) Regulations 2020.

36 The Online Safety Bill repeals the following existing legislative provisions which relate to communications offences:

a. Subsections (2)(a) and (b) of Section 127 of the Communications Act 2003 (improper use of electronic communications network), in so far as they extend to England and Wales; and

b. Subsections 1(1)(a)(ii), 1(1)(a)(iii), and 1(2) of the Malicious Communications Act 1988.

Territorial extent and application

37 Clause 180 and 181 set out the extra-territorial application and jurisdiction 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 United Kingdom, apart from a small number of exceptions:

a. The false and threatening communications offences, and the "cyberflashing" offence in Part 10 extend to England and Wales only; and

b. The flashing images offences in Part 10 extends to England, Wales, and Northern Ireland only).

38 The Bill also applies to providers of regulated services (as defined in clause 3(4)) which are based outside the United Kingdom. Extraterritorial application is necessary in order to fulfil the Bill's aim of protecting United Kingdom users online. Clauses 180 and 181 make provision in relation to the extra-territorial application of the Bill.

39 The Bill contains information offences. Clause 181 sets out that the offences apply to acts done by a person or individual (as applicable) in the United Kingdom or elsewhere.

40 Internet services policy is reserved across the United Kingdom, and as such the Government assesses that the Online Safety Bill is broadly reserved. Elements of the legislation interact with devolved competencies, and for a small number of provisions the UK Government will need to seek legislative consent from the Devolved Administrations (DAs).

a. The Bill confers power on Ministers in Scotland and Wales and the relevant department in Northern Ireland to amend the list of exempt educational institutions included at Schedule 1.

b. The Bill also confers a power on Ministers in Scotland to amend the list of CSEA offences included at Part 2 of Schedule 6. The Government is seeking legislative consent where these powers have been conferred.

41 The Bill also includes new communications offences in Part 10 relating to false and threatening communications. These currently apply to England and Wales and the UK Government will seek legislative consent for the application to Wales, alongside consent for any further extension to the Devolved Administrations.

42 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

43 The Bill is divided into 12 parts:

a. **Part 1** contains an overview clause, setting out what is included in this Bill.

b. **Part 2** contains definitions of the services to which the Bill applies.

c. **Part 3** imposes duties of care that apply to providers of regulated user-to-user and search services. It requires OFCOM to issue codes of practice relating to those duties.

d. **Part 4** imposes further duties on providers of regulated user-to-user and search services, including relating to user identity verification, CSEA content, and transparency reporting.

e. **Part 5** imposes duties on providers of regulated services that publish or display provider pornographic content.

f. **Part 6** imposes requirements on providers of regulated services to pay fees.

g. **Part 7** sets out OFCOM's powers and duties.

h. **Part 8** sets out the appeals and complaints procedures relating to regulated services.

i. **Part 9** sets out the Secretary of State's functions in relation to regulated services.

j. **Part 10** sets out new and updated communications offences.

k. **Parts 11 and 12** contain miscellaneous and general provisions. In particular, they define key concepts such as providers of regulated services, users, and internet services.

Part 1: Introduction

Clause 1: Overview of Act

44 The first clause sets out the subject matter of the various parts of the Bill.

Part 2: Key definitions

Clause 2: "User-to-user service" and "search service"

45 This clause provides definitions for the terms "user-to-user service" and "search service".

46 Subsection (1) defines a user-to-user service as an internet service which allows users to generate, upload or share content which may be encountered by others on that service. Subsection (2) sets out that it does not matter if content is shared with another user as long as a service has the functionality that allows such sharing. It also does not matter what proportion of content on a service is user-generated content.

47 Subsection (4) provides that a search service is an internet service which is, or includes a search engine. "Search engine" is defined in clause 201 as a service or functionality which enables a person to search more than one website or database.

48 Subsections (5) to (7) explain whether an internet service that both enables user-generated content and includes a search engine will be a user-to-user service or a search service. If the only user-generated content enabled by the service is of a kind exempted under the provisions of Schedule 1 to the Bill, then it will be a search service. If a search service enables other forms of user-generated content, then it will be a user-to-user service.

Clause 3: "Regulated service", "Part 3 service" etc

49 This clause defines the term "regulated service" and other related terms used in the Bill.

50 Subsection (2) sets out when user-to-user services and search services will be regulated user-to-user services and regulated search services. To be regulated, such services must have links with the United Kingdom and not be listed as exempt in Schedule 1 or Schedule 2. Subsection (3) states that these regulated user-to-user services and search services are referred to as Part 3 services in the Bill.

51 Subsection (4) defines "regulated service" as meaning a regulated user-to-user service, a regulated search service, and a service with links to the United Kingdom that publishes or displays provider pornographic content.

52 Subsections (5) and (6) clarify the circumstances under which a user-to-user or search service has links with the United Kingdom. A service will be in scope if it has a significant number of users in the United Kingdom or if the United Kingdom is a target market. A service will also be in scope if it can be used in the United Kingdom by individuals and there are reasonable grounds to believe that there is a material risk of significant harm to individuals in the United Kingdom. Subsection (4) in clause 71 applies an equivalent test to other internet services which publish or display provider pornographic content.

53 As the regulatory framework established by the Bill is focused on protecting individuals in the United Kingdom, these subsections ensure that services which do not have links to the United Kingdom are not in scope of regulation.

54 Subsection (7) provides that a regulated user-to-user service that includes a public search engine (i.e. one which is not an internal business service) is referred to as a "combined service".

Schedule 1: Exempt user-to-user and search services

55 Schedule 1 sets out which user-to-user and search services are exempt from regulatory duties. Subsection (2)(b)(i) of clause 3 ("Regulated service'", "Part 3 service" etc) states that services of the descriptions set out in this Schedule are not regulated user-to-user services or regulated search services.

56 Paragraphs 1 to 3 provide that services will be exempt if the only type of user-generated content enabled by the service is, respectively, email, SMS and/or MMS messages (as defined in clause 49(12)), or one-to-one live aural communications (as defined in clause 49(5)).

57 Under the limited functionality services exemption in paragraph 4, a user-to-user service is exempt if the only ways users can communicate on the service are the following:

a. The posting of comments or reviews on provider content (content published on the service by or on behalf of the service provider).

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

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

d. Displaying or producing identifying content (e.g. usernames or avatars) in connection with any of these activities.

58 This will exempt services where the only user interaction is, for example, 'below the line' content on media articles, or user reviews of directly provided goods and services. Any services that also have additional user-to-user functionalities will remain in regulatory scope.

59 Paragraph 5 sets out that a user-to-user service is also exempt if the only user-generated content it enables is of a kind covered by an exemption listed in paragraphs 1–4 (i.e. emails, SMS/MMS messages, one-to-one live aural communications, or comments and reviews relating to provider content).

60 However, paragraph 6 of Schedule 1 sets out that a service which would otherwise benefit from an exemption set out in the preceding paragraphs is not exempt if it has links with the United Kingdom and pornographic content is published or displayed on the service. If paragraph 6 applies to a service, paragraph 1 of Schedule 2 may exempt the service from the user-to-user service duties while keeping it in scope of the Part 5 duties.

61 Paragraph 7 exempts "internal business services". This exemption encompasses services such as business intranets, productivity and collaboration tools, content management systems, customer relationship management systems and database management software. To qualify as an internal business service, the service must meet the conditions set out in paragraph 7(2). Paragraph 8 provides details on internal business services where they make up only part of the user-to-user service or search service.

62 Paragraph 9 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 United Kingdom and bodies outside the United Kingdom where those services are provided in the exercise of functions of a public nature only.

63 Paragraph 10 provides an exemption for user-to-user or search services that are provided by education or childcare providers as described in Part 2, where those services are provided for the purpose of education and childcare.

64 Many education and childcare providers are subject to existing safeguarding duties which require them to protect children online. This exemption ensures that those education and childcare providers listed are not subject to oversight by both OFCOM and the relevant oversight bodies for education across the United Kingdom.

65 Paragraph 10(1) specifies a user-to-user service or a search service is exempt if the provider of the service is:

a. The responsible person for that education or childcare for e.g. a governing body of a maintained school in England.

b. A person employed or engaged to provide that education or childcare who is subject to safeguarding duties as defined in sub-paragraph (2), e.g. a teacher employed to work in an independent school in England.

66 Sub-paragraph (3) specifies that the responsible person must be a person who has day-to-day responsibility for the relevant education or childcare provision, for e.g. a governing body, rather than a person who may have a high-level duty to ensure education or child care is provided e.g. a Minister of a government department. A "person" includes (in addition to an individual and a body of persons corporate or unincorporate) any organisation or association of persons.

67 Schedule 1 Part 2 provides a list of descriptions of education and childcare provided in the United Kingdom that will be exempt under subsection 10. Any education or childcare providers not described in Part 2 will not be exempt under subsection 10.

68 Schedule 1 Part 3 provides a set of definitions for childcare, education, further education, higher education, primary education, and secondary education for each nation in the United Kingdom.

Schedule 2: User-to-user services and search services that include regulated provider pornographic content

69 Clause 3 (2)(b)(ii) provides that a user-to-user service or a search service is not a regulated user-to-user service or a regulated search service if it is a service of a kind described in Schedule 2. The effect of Schedule 2 is that certain user-to-user and search services which publish or display regulated provider pornographic content and which would otherwise be exempt under Schedule 1, are instead exempt from only the user-to-user and search services duties. Services which fall within Schedule 2 will still be in scope of Part 5 as set out in clause 71 and may therefore still be regulated services.

Clause 4: Disapplication of Act to certain parts of services

70 This clause sets out the circumstances in which this Bill does not apply to certain parts of regulated services because of the low risk of harm associated with them.

Part 3: Providers of regulated user-to-user services and regulated search services: Duties of care

Chapter 1: Introduction

Clause 5: Overview of Part 3

71 This clause provides an outline of each of the Chapters contained within Part 3 of the Bill.

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

User-to-user services: which duties apply, and scope of duties

Clause 6: Providers of user-to-user services: duties of care

72 This clause determines which of the duties set out in Part 3 apply to which regulated user-to-user services. The duties on search services are set out in the following chapter.

73 Subsection (2) lists the duties that all regulated user-to-user service providers must comply with.

74 Subsection (3) provides that providers of particular kinds of regulated user-to-user services will be required to comply with additional duties, as detailed in subsections (4) to (6).

75 Subsection (4) lists the additional duties that providers of regulated user-to-user services that are likely to be accessed by children must comply with. Whether or not a service is likely to be accessed by children is determined in accordance with clause 32.

76 Subsection (5) lists the additional duties that Category 1 services must comply with. Designation as a Category 1 service is determined by OFCOM's assessment under the provisions in clause 86.

77 Subsection (6) lists the additional duties that providers of combined services must comply with in relation to the search engine component of their service.

Clause 7: Scope of duties of care

78 Subsection (1) provides that the duties in this Chapter only apply to regulated user-generated content on user-to-user services that also include regulated provider pornographic content. Subsection (2) provides that the duties in this Chapter also do not apply to search content on combined services.

79 Subsection (3) provides that the duties in this Chapter only relate to the design, operation and use of a service in the United Kingdom and how it affects users in the United Kingdom.

Illegal content duties for all user-to-user services

Clause 8: Illegal content risk assessment duties

80 This clause sets out the risk assessment duties on all providers of regulated user-to-user services in relation to illegal content. Providers must carry out a suitable and sufficient risk assessment by the relevant deadline specified in Schedule 3.

81 Subsection (3) requires the service provider to keep the risk assessment up to date, including when OFCOM significantly changes a risk profile which applies to it.

82 Subsection (4) requires the service provider to carry out a further risk assessment before significantly changing the design or operation of the service.

83 Subsection (5) lists the factors that the service provider must assess, including several factors relating to the likelihood of users encountering illegal content or the service being used for the commission or facilitation of a priority offence, and the severity of the impact this would have on users. It requires the provider to take into account OFCOM's risk profiles (published under clause 89) relating to the kind of service it provides.

84 The findings of the provider's risk assessment, including its conclusions about the levels of risk, inform the steps it must take to comply with its safety duties to protect individuals from illegal content under clause 9.

85 OFCOM will have a duty under clause 90 to issue guidance to assist service providers to carry out their risk assessments.

Schedule 3: Timing of providers' assessments

86 Part 1 of Schedule 3 specifies the deadlines by which service providers must complete their illegal content risk assessments and children's access assessments.

87 The general approach is that service providers will have three months from the publication of the guidance relating to a particular assessment (or, once guidance has been published, from the date on which they become a service that needs to complete a particular assessment) to complete the relevant assessment. Part 2 of the Schedule specifies deadlines for children's risk assessments. Under Part 3 OFCOM may extend these deadlines for individual service providers or groups of service providers.

88 Part 3 of Schedule 3 sets out the deadlines by which risk assessments and child access assessments must be carried out by providers of video-sharing platform (VSP) services currently regulated by Part 4B of the Communications Act 2003. These services will be subject to transitional arrangements pursuant to which they will be obliged to undertake their risk and child access assessments before transitioning from the VSP regime to the Online Safety regime. The requirement to do the assessments is triggered by the assessment start date as set out in Schedule 3, paragraph 8. The general approach is that these services will have three months from the date that the requirement to conduct the assessments is imposed upon them or the date on which the guidance relating to a particular assessment is published, whichever is later.

Clause 9: Safety duties about illegal content

89 This clause sets out the duties on all providers of user-to-user services with regard to illegal content on their service.

90 Subsection (2) imposes a duty on providers to take proportionate measures relating to the design or operation of the service:

a. To prevent individuals from encountering priority illegal content by means of the service.

b. To mitigate and manage the risk (as identified in the most recent illegal content risk assessment carried out under clause 8) of the service being used for the commission or facilitation of a priority offence.

c. To mitigate and manage the risks of harm to individuals identified in the most recent illegal content risk assessment.

91 Subsection (3) requires service providers to use proportionate systems and processes designed to minimise the length of time for which any priority illegal content is present on their services and ensure that any illegal content is swiftly taken down once they become aware of its presence.

92 Subsection (4) provides that the duties in subsections (3) and (4) apply to the way the service is designed, operated and used, as well as to the content present on it. This subsection also lists areas within which the service provider may be required to take or use measures, if proportionate, to comply with their illegal content safety duties. These areas include arrangements for compliance and risk management, service design including design of algorithms (e.g. changing the design of algorithms to prevent users from being directed to illegal content), policies on access and use (e.g. preventing repeat offenders using their services), content moderation (e.g. content removal), user empowerment and support measures and staff policies.

93 Subsections (5) and (6) impose obligations on providers to state in their terms of service how individuals are to be protected from illegal content and to apply these consistently.

94 Subsection (7) specifies that the service provider must include information in its terms of service about any proactive technology that it will use to comply with its duties in respect of illegal content.

95 Subsection (8) sets out that the terms of service must be clear and accessible.

96 Subsection (9) specifies the factors which are particularly relevant for determining whether measures, systems and processes to comply with illegal content duties are proportionate. The factors are findings of the most recent risk assessment (including the identified levels of risk) and the service provider's size and capacity. In practice, this means that the requirements for proportionality will be different for a large, high risk service compared to a small, low risk service. It also means that service providers need to design their systems in a way that reflects the risk of illegal content being present on their service.

97 Subsection (11) signposts the fact that the duties about users' rights to freedom of expression and privacy in clause 18 are relevant to the illegal content safety duty in this clause.

User-to-user services likely to be accessed by children

Clause 10: Children's risk assessment duties

98 This clause sets out the children's risk assessment duties for user-to-user services that are likely to be accessed by children.

99 Subsection (5) requires service providers to notify OFCOM about content they identify that is harmful to children that is not specified in secondary legislation as primary priority or priority content that is harmful to children, as well as the incidence of such content on the service.

100 Subsection (6) lists the factors that the service provider must assess, for example risks created by algorithms and how easily and quickly content can be shared - such as features which automatically feed content to a user. This subsection requires the provider to take into account the risk profile (which would be published by OFCOM under clause 89) that relates to the kind of service it provides.

101 OFCOM will have a duty under clause 90 to issue guidance to assist service providers to carry out their children's risk assessments.

Clause 11: Safety duties protecting children

102 This clause sets out the duties on providers of user-to-user services with regard to content that is harmful to children but is not illegal. User-to-user services that are likely to be accessed by children (see clause 32) must comply with these duties.

103 Subsection (2) imposes a duty on service providers to take proportionate steps relating to the design and operation of the service:

a. To mitigate and manage the risk of harm to children in different age groups from risks identified in the most recent children's risk assessment carried out under clause 10.

b. To mitigate the impact of harm to children in different age groups from content that is harmful to children. This could include user support measures, such as signposting child users to sources of support if they have experienced harm on the service.

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

a. Prevent children of any age from accessing primary priority content (as defined in regulations to be made under clause 55) on their service. This could be achieved by using age verification.

b. Protect children in age groups which are judged to be at risk from other content that is harmful to children (either priority content as defined in regulations made under clause 55 or other content that satisfies the definition of content that is harmful to children in clause 54(4)(c)) on their service.

105 The duties described in subsections (2) and (3) apply to all areas of the service, including the way the service is designed, operated and used, as well as to the content present on it.

106 Subsection (4) references age assurance as an example of a measure which providers may use to identify who is a child user, or which age group a child user is in, to meet the duties under subsection (2) and (3). Subsection (5) also lists areas within which the service provider may be required to use measures, if proportionate, to comply with the safety duties for protecting children. These areas include arrangements for compliance and risk management, service design, policies on access and use (e.g. preventing children from accessing specific content on the service), content moderation (e.g. content removal), user empowerment and support measures and staff policies.

107 Subsection (6) requires providers to state in their terms of service how children are being prevented from encountering primary priority content and protected from encountering priority content on their service. It also requires providers to set out how children are protected from encountering other content that would satisfy the definition of content that is harmful to children in clause 54. These terms must be applied consistently and must be clear and accessible (subsections (7) and (10)).

108 Subsection (8) specifies that where a provider prevents access to part of, or the whole of the service for users under a particular age, it is required to set out in its terms of service the measures it uses to do so. It is also required to apply those provisions consistently.

109 Subsection (9) specifies that information about any proactive technology the service provider will use to comply with its duties under subsections (2) and (3) must be included in the terms of service.

110 Subsection (11) specifies that the factors (in particular) which determine whether steps, systems and processes are proportionate are findings of the most recent children's risk assessment (including levels of risk) and the service provider's size and capacity.

111 Subsection (12) makes clear that services are only required to fulfil the duty in this clause in relation to the kinds of non-designated content (i.e. content that is neither primary priority content nor priority content but which would satisfy the test of being harmful to children in clause 54(4)(c)) if risks from such content have been identified in the most recent children's risk assessment.

112 Subsection (13) 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 its most recent children's risk assessment.

113 Subsection (14) provides that the duties in subsections (3) and (6) (which require service providers to take steps to prevent or protect children from encountering harmful content and to specify those steps in their terms of service) apply only in relation to content which gives rise to a risk of harm due to its nature. It would not be feasible for providers to fulfil these duties for content that is only harmful by the fact of its dissemination. An example would be doxxing, where the content is not inherently harmful to children encountering it but its dissemination may be harmful to a particular targeted child. However, under subsection (2)

companies have a duty to mitigate and manage the risks of harm to children on their service, including harm caused through the dissemination of content.

114 Subsections (15) and (16) clarify that the duties to protect children which are set out in this clause only extend to those parts of the service which it is possible for children to access. 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. The safety duties would not apply to those parts of the service.

115 Subsection (18) signposts the fact that the duties about users' rights to freedom of expression and privacy in clause 18 are relevant to the safety duties for services likely to be accessed by children in this clause.

Clause 12: User empowerment duties

116 This clause sets out the duty on providers of Category 1 services to provide adult users with the features to increase their control over certain categories of content, as set out in subsections (10), (11) and (12) and who they interact with.

117 Under subsection (2) and (3), providers of Category 1 services will need to have features in place to allow adult users control over content to which this subsection applies. When users decide to use these features, Category 1 services will need to apply systems and processes which are effective in limiting users' exposure to certain kinds of content. This content is set out within this clause in subsections (10), (11) and (12). There should either be a reduced likelihood of users seeing this kind of content, or users should be alerted to the nature of the content.

118 Under subsection (6) and (7) providers of Category 1 services will also need to provide users with tools to filter content from non-verified users. This includes ensuring that a user is able to set a preference preventing non-verified users from interacting with their content, and reducing the likelihood of them encountering content from a non-verified user.

119 The duty on Category 1 services in subsection (2) to offer adult users greater control over the kind of content they engage with is a proportionate duty. Subsection (8) sets out relevant criteria for determining proportionality, this is the likelihood that users will encounter the specified categories of content on the service, and the size and capacity of a service provider.

120 Subsection (9) sets out the requirements for content to be in scope of subsection (2). It must be regulated user generated content on the service in question and content in subsections (10), (11) and (12).

121 Subsections (10), (11) and (12) set out the kinds of content that the user empowerment content features under subsection (2) and (3) apply to. The kinds of content that are covered are: content that encourages, promotes or provides instructions for suicide or an act of deliberate self-injury, or an eating disorder; and content that is abusive or incites hate on the basis of race, religion, sex, sexual orientation, disability, or gender reassignment. These definitions do not capture mere discussion of these topics. Subsection (13), (14) and (15) define the meanings of terms contained within this clause.

Clause 13: Duties to protect content of democratic importance

122 This clause sets out the duties on providers of Category 1 services to protect content of democratic importance on their services.

123 Subsection (2) places a duty on providers of Category 1 services to take into account the importance of freedom of expression when designing proportionate systems and processes for taking decisions about content of democratic importance or about users who post such content. This includes decisions about whether to take the content down, to restrict access to it or to take action against a user of the service. For example, providers of Category 1 services could adopt processes to identify democratically important content and ensure users have access to this, even where it might otherwise be voluntarily removed (i.e. for non-compliance with the providers own terms of service, rather than as otherwise required by the Bill's safety duties).

124 Subsection (3) requires providers to apply these systems and processes in the same way to a wide diversity of political opinion. This is to ensure that providers of Category 1 services do not privilege some political opinions over others when deciding how to protect content of democratic importance.

125 Subsection (4) requires providers to set out in terms of service the policies and processes designed when complying with subsection (2).

126 Subsection (5) requires that these terms of service are clear and consistently applied. The intention is that the terms of service should be easily understandable for users and that similar decisions are taken about the treatment of similar pieces of content.

127 Subsection (6) defines "content of democratic importance" as news publisher content or regulated user-generated content, both defined under clause 49, which is, or appears to be, specifically intended to contribute to democratic political debate in the United Kingdom or in any part or area of the United Kingdom. Examples of such content would be content promoting or opposing government policy and content promoting or opposing a political party.

Clause 14: Duties to protect news publisher content

128 This clause places a duty on Category 1 service providers to take certain steps with regard to recognised news publishers, as defined by the Bill, before removing or moderating their content or taking action against their account.

129 Subsection (3) sets out the steps the service must take before removing or moderating content or taking action against a recognised news publishers' account. This includes notifying the news publisher of the intention to take a particular action. This notification must be in writing (as set out in clause 207). The notification must also set out reasons for any proposed action by referring to specific, relevant provisions of the service's own terms of service.

130 Subsections (4) and (5) set out certain circumstances where a provider can take action in relation to recognised news publisher content without following the steps at subsection (3). These are if the service reasonably considers that continuing to host the content in question

would give rise to criminal or civil liability for the service or where the content amounts to a relevant offence as defined by the Bill. Subsections (10) and (11) require that judgements about whether content amounts to a relevant offence must be taken as per clause 170, and that OFCOM's guidance as per clause 171 is also relevant.

131 Subsection (7) sets out the steps the service must take if it takes action in relation to recognised news publisher content without taking the steps set out at subsection (3). The notification must be in writing.

132 Subsection (8) specifies that if a recognised news publisher has already been banned from using a service either before the regulatory framework came into force, or after the process in (3) has been followed, and the ban is still in force, the service may take action against its content without following the steps at subsection (3) and (7). This provision does not enable Category 1 service providers to ban a recognised news publisher once the regulatory framework is in force without following the process in subsection (3) in the first instance.

133 Subsection (9) specifies the circumstances where a service should not be regarded as taking action in relation to recognised news publisher content. This applies where a service takes action against content that is not recognised news publisher content, but such content is impacted and it is not feasible for the service to separate the recognised news publisher content; and where a service takes action against an account and that action impacts recognised news publisher content that has been uploaded or shared by the relevant user.

134 Subsection (13) defines 'taking action' in relation to content. This covers any action taken in relation to specific pieces of content which is intended to remove content, restrict users access to it, or to warn users about it. It is not intended to include actions to do with personalised content curation; for example, personalised recommendations based on users' preferences.

Clause 15: Duties to protect journalistic content

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

136 Subsection (2) places a duty on providers of Category 1 services to take into account the importance of free expression when designing proportionate systems and processes for taking decisions about journalistic content, or about users who post such content. This includes decisions about whether to take the content down, to restrict access to the content or to take action against a user of the service. For example, providers of Category 1 services could adopt procedures to identify journalistic content and ensure users have access to this, even where it might otherwise be voluntarily removed (i.e. for non-compliance with the providers own terms of service, rather than as otherwise required by the Bill's safety duties).

137 Subsection (3) and (4) require providers of Category 1 services to create a dedicated complaints procedure available to users who generate, upload or share journalistic content on the service and to creators of journalistic content. The procedure must allow users and creators (as defined in subsections (12) and (13)) to challenge decisions to take down or restrict access to journalistic content or to take action against a user because of journalistic content

shared, uploaded or generated by the user. The complaints procedure must be expedited. Under subsection (5), if a complaint is upheld, the content must be swiftly reinstated or the action against the user swiftly reversed. These subsections also make clear that providers are not required to make this complaints procedure available to a recognised news publisher in relation to any decision the provider has taken when complying with their duties set out in clause 14.

138 Subsection (8) requires that the terms of service about journalistic content are clear and consistently applied. The intention is that the terms of service should be easily understandable for users and that similar decisions are taken about the treatment of similar pieces of content.

139 Subsection (9) defines "journalistic content" for the purposes of Part 3 of the Bill as covering both news publisher content and regulated user-generated content, defined in clause 49, that is generated for the purposes of journalism, and which is 'UK-linked'. This includes, but is not limited to, content generated by news publishers, freelance journalists and citizen journalists. Subsection (9) defines the term "UK-linked".

Duties about content reporting and complaints procedure

Clause 16: Duty about content reporting

140 This clause sets out the content reporting mechanisms which providers of regulated user-to-user services must have in place (clause 26 contains similar provisions relating to search services).

141 All providers of user-to-user services must enable users and other affected persons (as defined in subsection (5)) to report illegal content, providers of services likely to be accessed by children must enable reporting of content that is harmful to children where they are able to access such content. The types of content that users and affected persons must be able to report correspond to the types of content that the regulatory framework requires them to address.

142 Subsection (5) lists the types of people who might be affected by content, or who may need to assist other users with making a complaint, but who might not be users of the service themselves. These people must also be able to access the content reporting mechanisms.

Clause 17: Duties about complaints procedures

143 This clause sets out the duties regarding complaints and redress mechanisms which apply in relation to providers of regulated user-to-user services (clause 27 contains similar provisions relating to search services).

144 Subsection (2) sets out that services must have a complaints procedure that:

a. allows for complaints to be made relevant to the type of content and the duties on the service.

b. provides for appropriate action to be taken when a complaint is upheld. Examples of appropriate action might include removal of illegal content if flagged, or reinstating content unfairly removed.

c. is easy to access and use, including by children, and that the process is transparent. For example, each step of the complaints procedure should be set out clearly, including the types of complaints that can be made by users or other "affected persons" (which subsection (7) indicates has the meaning given in clause 17(6)) and what they can expect to happen from the point at which they make the complaint.

145 Subsection (3) sets out that the policies and procedures that govern handling of complaints must be set out in a service provider's terms of service, and these must be easily accessible, including for children. This is to ensure that users and affected persons can easily find and use the complaints policies and procedures.

146 Subsections (4) to (6) set out the types of complaints for which the different categories of service provider must have a complaints procedure. The types of complaint correspond to the types of content that the regulatory framework requires them to address.

Cross-cutting duties

Clause 18: Duties about freedom of expression and privacy

147 This clause sets out the freedom of expression and privacy duties. This clause applies in relation to user-to-user services (clause 28 contains similar provisions relating to search services).

All services

148 Subsection (2) places a duty on providers of all regulated user-to-user services to have particular regard to the importance of protecting users' legal rights to freedom of expression when deciding on and implementing safety measures to comply with their duties. Examples of measures that services could take to comply with this duty could include ensuring human moderators are adequately trained to assess contextual and linguistic nuance to prevent over-removal of content.

149 Subsection (3) places a duty on providers of all regulated user-to-user services to have particular regard to the importance of protecting users from breaches of law concerning privacy when deciding on and implementing safety measures to comply with their duties. This is intended to encompass breaches of existing statutory provisions in data protection legislation such as the Data Protection Act 2018 and the Privacy and Electronic Communications Regulations 2003, as well as common law rights such as those relating to private and confidential information. The regulator which enforces obligations which arise under data protection law is the Information Commissioner's Office.

150 Service providers can comply with their duties in subsections (2) and (3) by following measures in OFCOM's codes of practice (see clause 44(2)). Under Schedule 4 paragraph 10, OFCOM are required to design recommended measures in light of the importance of protecting users' rights to freedom of expression and protecting users' privacy, and where appropriate, OFCOM should incorporate protections for the same. Where service providers take measures different from those set out in the codes of practice, they are also under an obligation to ensure that they have particular regard to the importance of freedom of

expression and user privacy (see clause 44(5)). OFCOM are obliged to consult with the Information Commissioner's Office when preparing the codes of practice (see clause 36(6)(g)).

Category 1 services

151 Subsection (4) requires providers of Category 1 services to carry out and publish an impact assessment on the impact that any steps which they have taken, or plan to take, to comply with their safety duties have, or will have, on users' rights to freedom of expression and users' privacy. They must also publish a statement specifying any positive steps they have taken to protect users' rights to freedom of expression and privacy in response to this impact assessment (subsection (7)). Subsection (5) requires this impact assessment to consider the effect of their safety measures and policies on the availability and treatment of news publisher content and journalistic content.

152 Subsection (9) clarifies that the use of "safety measures and policies" in this section refers to those designed to secure compliance with (a) clause 9 (illegal content), (b) clause 11 (children's online safety), (c) clause 12 (user empowerment), (d) clause 16 (content reporting), or (e) clause 17 (complaints procedures).

Clause 19: Record-keeping and review duties

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

154 Providers of user-to-user services are obliged to keep a written record of the risk assessments that they carry out. They must also keep written records explaining which of the measures recommended in a code of practice they are taking for the purposes of complying with the duties listed in subsection (9). Where a provider is taking an alternative approach to that recommended in a code of practice, it must keep a written record explaining what it is doing instead and how that amounts to compliance with the relevant duties.

155 Subsection (6) requires providers to review compliance with the relevant duties regularly and after making any significant change to their service.

156 Subsection (7) provides OFCOM with the ability to exempt categories of providers from the need to keep written records and carry out reviews. It is anticipated that this power could be used for small, low risk services to ensure these service providers do not face an unnecessary regulatory burden. Where OFCOM considers an exemption is no longer appropriate, they may revoke that exemption. Under subsection (8), OFCOM must publish the details of any such exemptions or revocation of exemptions with reasons.

Chapter 3: Providers of search services: duties of care

Search services: which duties apply, and scope of duties

Clause 20: Providers of search services: duties of care

157 This clause lists (in subsection (2)) the duties which apply to all providers of regulated search services and (in subsection (3)) the additional duties that providers of search services that are

likely to be accessed by children must comply with. Whether or not a service is likely to be accessed by children is determined by the service provider in accordance with clause 32.

Clause 21: Scope of duties of care

158 Subsection (1) of this clause sets out how the duties in Part 3, Chapter 3 apply to providers of a search service. The duties for providers of a search service only extend to the design, operation and use of the service in the United Kingdom or how the service affects users and others (such as individuals affected by content on services they do not themselves use) in the United Kingdom.

159 Subsection (2) sets out how the duties in the Chapter apply to the search engine of a combined service. Firstly, where duties in this Chapter require a service to include something in a publicly available statement, the provider of a combined service may set this out in terms of service. Unlike a search service, a combined service has a user-to-user part which will have such terms. Secondly, since the duties in this chapter refer to a "search service" and a "provider of a search service", this provision makes clear that these references are also to the search engine of a combined service (which does not fulfil the definition of a search service). The intention is that duties apply to the search engine of a combined service, and to the provider of that service, in the same way that they apply to a search service and its provider. The references in clause 20 are excepted from this provision because the duties on the provider of a combined service in relation to its search engine are set out at clause 6(6).

Illegal content duties for all search services

Clause 22: Illegal content risk assessment duties

160 This clause sets out the risk assessment duties on all providers of regulated search services in relation to illegal content. Providers must carry out a suitable and sufficient risk assessment by the relevant deadline specified in Schedule 3 and keep this up to date.

161 Subsection (4) requires the service provider to carry out a further risk assessment before significantly changing the design or operation of the service such that the impact of the proposed change is assessed.

162 Subsection (5) lists the factors that the service provider must assess, including several factors relating to the likelihood of users encountering illegal content and the severity of the impact this would have on users. It requires the provider to take into account OFCOM's risk profiles (published under clause 89) relating to the kind of service it provides when doing so.

163 The findings of the provider's risk assessment, including its conclusions about the levels of risk, inform the steps it must take to comply with its safety duties to protect individuals from illegal content under clause 23.

164 OFCOM have a duty under clause 90 to issue guidance to assist service providers with carrying out their risk assessments.

Clause 23: Safety duties about illegal content

165 This clause imposes duties on providers of regulated search services in respect of illegal content. Subsection (2) requires service providers to take proportionate steps relating to the design or operation of the service to mitigate and manage the risks of harm to individuals, as identified in the most recent illegal content risk assessment of the service under clause 22.

166 Subsection (3) requires service providers to ensure that 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. These systems and processes could include, for example, down-ranking illegal content in search results, ensuring predictive searches do not drive users towards illegal content, and signposting users who search for illegal content towards resources and support.

167 Subsection (4) provides that these duties apply to the way the service is designed, operated and used, as well as to the content present on it. This subsection also lists areas in which the service provider is required to use measures, if it is proportionate to do so, to comply with its illegal safety duties.

168 Subsections (5), (6) and (8) require service providers to set out their policies and procedures for protecting users from illegal content in a clear and accessible publicly available statement and apply them consistently.

169 Subsection (7) specifies that the service provider must include information in a publicly available statement about any proactive technology that it will use to comply with its duties in respect of illegal content.

170 Subsection (9) specifies the factors which are particularly relevant for determining whether measures, systems and processes to comply with the illegal content duties are proportionate. These factors are the findings of the most recent risk assessment (including levels of risk) and the service provider's size and capacity. In practice, this means that the requirements will be different for a large, high risk service compared to a small, low risk service. It also means that service providers need to design their systems in a way that reflects the risk of their search content containing illegal content.

Search services likely to be accessed by children

Clause 24: Children's risk assessment duties

171 This clause sets out the children's risk assessment duties for providers of search services that are likely to be accessed by children. Service providers must carry out a suitable and sufficient children's risk assessment by the relevant deadline specified in Schedule 3 and keep this up to date.

172 Subsection (5) lists the factors that the service provider must assess in the children's risk assessment and requires it to take into account the risk profile that relates to the kind of service it provides.

173 OFCOM will have a duty under clause 90 to issue guidance to assist service providers to carry out their children's risk assessments.

Clause 25: Safety duties protecting children

174 This clause sets out the duties on providers of regulated search services with regard to content that is harmful to children but is not illegal. All providers of regulated search services that are likely to be accessed by children must comply with these duties.

175 Subsection (2) requires service providers to take proportionate steps relating to the design or operation of the service. These service providers must mitigate and manage the risks and impact of harm to children in different age groups, which they need to have identified in their most recent children's risk assessment of the service under clause 24.

176 Subsection (3) requires service providers to ensure they have proportionate systems and processes to minimise the risk of children encountering primary priority content that is harmful to children or other content that is harmful to children in certain age groups. These systems and processes could include, for example: down-ranking content that is harmful to children in search results displayed to child users; ensuring predictive searches do not drive children towards harmful content; and signposting children who search for harmful content towards resources and support.

177 Subsection (4) provides that these duties apply to the way the service is designed, operated and used, as well as to the content that may be accessed via search results. This subsection also lists areas in which the service provider is required to use measures to comply with its child safety duties, if it is proportionate for them to do so.

178 Subsections (5), (6) and (8) require service providers to set out their policies and procedures for protecting children from harmful content in a clear, accessible and publicly available statement, and apply them consistently.

179 Subsection (7) specifies that the service provider must include information in a publicly available statement about any proactive technology that it will use to comply with its safety duties for children.

180 Subsection (9) specifies the factors which determine whether steps, systems and processes are proportionate. This includes the findings of the most recent children's risk assessment (including levels of risk) in particular, as well as the service provider's size and capacity. In practice, this means that the requirements will be different for a large, high risk service compared to a small, low risk service.

181 Subsection (10) specifies that service providers are only required to meet a duty in this clause in relation to non-designated content that is harmful to children if risks from such content have been identified in the most recent children's risk assessment. Non-designated content is that which is neither primary priority content nor priority content but which would satisfy the test of being harmful to children in clause 54(4)(c)).

182 Subsection (13) clarifies that the duties in this clause 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 30. 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.

Duties about content reporting and complaints procedures

Clause 26: Duty about content reporting

183 This clause sets out the content reporting mechanisms which apply in relation to all providers of regulated search services (see clause 16 for the equivalent provisions relating to user-to-user services).

184 Subsection (2) places a duty on providers of services to have systems and processes in place that allow users and affected persons (as defined in subsection (5)) to report content of the kinds listed which are relevant to the service in question.

Clause 27: Duties about complaints procedures

185 This clause sets out the duties regarding complaint and redress mechanisms which apply in relation to all providers of regulated search services as set out in clause 20 (see clause 6 for the provisions relating to user-to-user services).

186 Subsection (2) sets out the requirements on services' complaints procedures. Subsection (3) sets out that the policies and procedures that govern handling of complaints must be set out in a service provider's terms of service, and that these must be accessible for all users, including children. This is to ensure that users and affected persons can easily find and use the complaints policies and procedures.

187 Subsection (4) sets out the types of complaints that can be made to all search services.

188 Subsection (5) sets out the types of complaints that can be made to search services likely to be accessed by children.

Cross-cutting duties

Clause 28: Duties about freedom of expression and privacy

189 This clause sets out the freedom of expression and privacy duties that apply in relation to all providers of search services (see clause 18 for the equivalent provisions relating to user-to-user services).

190 Subsection (2) places a duty on all providers of search services to have particular regard to the importance of protecting users' and interested persons' legal rights to freedom of expression when deciding on and implementing steps to comply with their safety duties.

191 Subsection (3) places a duty on providers of all regulated search services subject to the safety duties to have particular regard to the importance of protecting users from breaches of law concerning their privacy when deciding on and implementing safety measures to comply with their duties. This is intended to encompass existing obligations on service providers regarding

users' privacy under data protection law, in particular the Data Protection Act 2018 and the Privacy and Electronic Communications Regulations 2003, as well as common law rights such as those relating to private and confidential information. The regulator which enforces obligations which arise under data protection law is the Information Commissioner's Office.

192 Service providers can comply with duties in subsections (2) and (3) by following steps in OFCOM's codes of practice. Under Schedule 4 paragraph 10, OFCOM are required to design recommended steps to be included in codes of practice in light of the importance of protecting users' legal rights to freedom of expression and protecting users' privacy, and, where appropriate, they should incorporate protections for the same. Where service providers take alternative measures to those set out in the codes of practice, they are also under an obligation to ensure that they have particular regard to the importance of freedom of expression and user privacy. OFCOM are obliged to consult with the Information Commissioner's Office when preparing the codes of practice (see clause 36(6)(g)).

Clause 29: Record-keeping and review duties

193 This clause sets out the record-keeping and review obligations that apply to providers of regulated search services.

194 Providers of regulated search services are obliged to keep a written record of the risk assessments that they carry out. They must also keep written records explaining which of the measures recommended in a code of practice for the purposes of complying with the duties listed in subsection (9) they are taking. Where a provider is taking an alternative approach to that recommended in a code of practice, it must keep a written record explaining what it is doing instead and how that amounts to compliance with the relevant duties.

195 Subsection (6) requires providers to review compliance with the relevant duties regularly and after making any significant change to their service.

196 Subsection (7) provides OFCOM with the ability to exempt categories of providers from the need to keep written records and carry out reviews. It is anticipated that this power could be used for small, low risk services to ensure these service providers do not face an unnecessary regulatory burden. Where OFCOM consider an exemption is no longer appropriate, they may revoke that exemption. Under subsection (8), OFCOM must publish the details of any such exemptions or revocation of exemptions with reasons.

Chapter 4: Children's Access Assessments

Clause 30: Children's access assessments

197 This clause establishes a requirement for providers of regulated services to assess whether it is possible for children to access the service (or part of it) and, if so whether a significant number of children use the service (or the relevant part) and/or whether the service (or relevant part) is likely to attract a significant number of users who are children. Where either of the latter two conditions is satisfied, the service provider will be obliged to conduct a children's risk assessment (see clauses 10 and 24) and will be subject to the safety duties protecting children (see clauses 11 and 25).

198 Subsection (2) specifies 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 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 is intended to refer to the age assurance measures that provide the highest level of confidence about a user's age.

199 A provider is only required to consider parts of its service that are user-to-user services or search services when assessing the likelihood of children's access.

Clause 31: Duties about children's access assessments

200 This clause explains when children's access assessments must be carried out. It also specifies that children's access assessments must be suitable and sufficient and that providers must make and keep a written record of each assessment.

201 Providers must also carry out a separate children's access assessment for each of the services they provide, as specified at subsection (5).

Clause 32: Meaning of "likely to be accessed by children"

202 This clause sets out three cases in which a regulated Part 3 service is to be considered "likely to be accessed by children" and therefore subject to the children's risk assessment and child safety duties at either clauses 10 and 11 (for regulated user-to-user services) or 24 and 25 (for regulated search services).

203 The first case at subsection (2) is when it is both possible for children to access the service and the "child user condition" (referred to in clause 31(3)) is met in relation to the service as a whole, or any part of the service which it is possible for children to access.

204 The second case at subsection (3) is when the service provider has failed to complete the first children's access assessment required under clause 32(1).

205 The third case at subsection (6) is when, following an investigation into a provider's failure to comply with a duty about children's access assessments, OFCOM concludes that a service should be treated as "likely to be accessed by children". Clause 123(4) and (5) empowers OFCOM to give a confirmation decision to a provider if it is satisfied that the provider has failed to comply with such duties.

Chapter 5: Duties about fraudulent advertising

Clause 33: Duties about fraudulent advertising: Category 1 services

206 This clause sets out duties about fraudulent advertising for providers of Category 1 services. Category 1 service providers must operate their services using proportionate systems and processes designed to prevent individuals from encountering fraudulent advertisements, minimise the amount of time that fraudulent advertising is present, and swiftly remove fraudulent advertising once they are made aware of it through any means. The definition of a fraudulent advertisement to which the duties on providers apply is at subsection (3).

207 Subsection (2) specifies that a Category 1 service provider must include information in its terms of service about any proactive technology that it will use to comply with its duties in respect of fraudulent advertising.

208 Subsection (4) specifies that if a person is the provider of more than one Category 1 service, the duties set out in this clause apply in relation to each such service.

209 Subsection (5) sets out factors for determining proportionality regarding service providers' systems and processes to comply with the duty about fraudulent advertising. These are a) the nature and severity of potential harm from fraudulent advertisement and b) the degree of control a provider has over the placement of advertisements on the service. This recognises that a provider of a Category 1 service may rely on third party intermediaries to display paid advertisements on its service, and will therefore have less control over measures to prevent posting of fraudulent adverts.

Clause 34: Duties about fraudulent advertising: Category 2A services

210 This clause sets out the fraudulent advertising duties for providers of Category 2A[11] services. Category 2A service providers must operate their services using proportionate systems and processes designed to prevent individuals encountering fraudulent advertisements in or via search results of the service, minimise the amount of time that fraudulent advertising is present, and swiftly remove fraudulent advertising once they are made aware of it through any means. A fraudulent advertisement to which the duties on providers apply is defined in subsection (3).

211 Subsection (2) specifies that a Category 2A service provider must include information in a publicly available statement about any proactive technology that it will use to comply with its duties in respect of fraudulent advertising.

212 Subsection (4) defines what is meant by references to encountering fraudulent advertisements "in or via search results" of a search service. This includes interacting with a paid-for advertisement in search results, for example by clicking on the fraudulent advertisement in a search result and then being redirected to a web page which was linked to the original fraudulent advertisement. Encountering does not extend to any subsequent interactions with a website, for example leaving the original fraudulent advertisement web page.

213 Subsection (5) specifies that if a person is the provider of more than one Category 2A service, the duties set out in this clause apply in relation to each such service.

214 Subsection (6) sets out factors for determining proportionality regarding service providers' systems and processes to comply with the duty about fraudulent advertising. These are a) the nature and severity of potential harm from fraudulent advertisement and b) the degree of control a provider has over the placement of advertisements on the service. This recognises that a Category 2A service provider may rely on third party intermediaries to display paid

[11] 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.

advertisements on its service, and will therefore have less control over measures to prevent the posting of fraudulent adverts.

Clause 35: Fraud etc offences

215 This clause sets out a list of offences that will constitute fraud offences in relation to the duties about fraudulent advertising.

216 Subsection (5) states that the relevant inchoate offences also apply to the definition of fraud offences e.g. attempting or conspiring to commit an offence specified in subsection (2), (3) or (4).

Chapter 6: Codes of practice and guidance

Codes of practice

Clause 36: Codes of practice about duties

217 OFCOM are required to produce specific codes of practice in relation to the illegal content duties (set out in clauses 9 and 23) covering terrorist content and offences (subsection (1)) and child sexual exploitation and abuse content and offences (subsection (2)).

218 Subsection (3) requires OFCOM to produce 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 relevant duties. The relevant duties are listed in subsection (10).

219 Subsection (4) sets out that OFCOM must produce a code of practice for providers of Category 1 and Category 2A services in relation to the duties set out in Chapter 5 (duties about fraudulent advertising).

220 Subsection (5) allows OFCOM to produce amendments and replacements to the codes of practice or to withdraw a code of practice.

221 When preparing draft codes of practice or amendments to them, subsection (6) sets out the parties whom OFCOM must consult. In preparing certain codes of practice, OFCOM must also consult those with expertise in national security or the enforcement of criminal law which is relevant to online safety matters (subsection (7)). Subsection (8) sets out the codes of practice to which this consultation requirement applies.

222 Subsection (9) sets out that the consultation requirements in subsections (6) and (7) are subject to exceptions where minor amendments are made to the codes of practice (as set out in clause 43).

Clause 37: Codes of practice: principles, objectives, content

223 This clause introduces Schedule 4 which establishes the principles OFCOM must consider when preparing codes of practice, the online safety objectives and the measures that may be recommended by codes of practice. It also contains other provisions related to codes of practice.

Schedule 4: Codes of practice under section 36: principles, objectives, content

224 Paragraph 1 requires OFCOM to consider how appropriate the provisions of codes of practice are for the different kinds of regulated user-to-user and search services and to the differing sizes and capacities of the providers of those services.

225 Paragraph 2 sets out various principles OFCOM must have regard to when preparing or amending a code of practice.

226 Paragraph 3 requires OFCOM to ensure that the measures set out in its codes of practice are compatible with the online safety objectives, which are set out at paragraph 4 for regulated user-to-user services and paragraph 5 for regulated search services.

227 Paragraph 6 clarifies how the objectives for user-to-user services and search services apply to combined services.

228 Paragraph 7 gives the Secretary of State power to make changes to the online safety objectives by regulations subject to the affirmative resolution procedure. Paragraph 8 obliges OFCOM to consider as soon as is reasonably practicable whether they should review and subsequently amend the codes of practice following changes to the online safety objectives.

229 Paragraph 9 imposes obligations on OFCOM relating to the content of their codes of practice. These are that codes of practice for illegal content and children's online safety must include measures in the areas set out in those duties where this is proportionate to the type and size of service providers and to risk (sub-paragraph (5)). Sub-paragraphs (1) and (2) cover user-to-user services and (3) and (4) cover search services.

230 Paragraph 10 requires OFCOM to design measures in the codes of practice in the light of the principles of the importance of protecting users' rights to freedom of expression and privacy, and to incorporate safeguards for these rights where appropriate.

231 Paragraph 11 provides that measures set out in a code of practice may only apply to services that are in the United Kingdom or affect users in the United Kingdom. This means that OFCOM could not set out measures in codes of practice that apply to services that do not operate in the United Kingdom or have United Kingdom users.

232 Paragraph 12 sets constraints on how OFCOM may recommend proactive technologies in the codes of practice relating to illegal content, child online safety and fraudulent advertising. Any such recommendation must be a proportionate response to the risk. In relation to the accuracy and effectiveness of tools, OFCOM may refer to industry standards or set principles through the codes. A proactive technology measure may not be recommended to analyse user-generated content, or metadata relating to such content, which has been communicated privately.

233 Paragraph 13 allows codes of practice to make provisions that are different for user-to-user and search services and to make different provisions for different kinds of service. It also allows OFCOM to differentiate between services and service providers as appropriate.

234 Paragraph 14 provides that codes of practice can apply to service providers based outside of the United Kingdom.

235 Paragraph 15 specifies that a code of practice for the purposes of this schedule means a code of practice about duties issued by OFCOM under clause 36.

Clause 38: Procedure for issuing codes of practice

236 This clause sets out the procedural requirements for approval of the draft codes of practice.

237 Subsections (1) and (2) set out that OFCOM must submit a draft 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 39), the Secretary of State must lay the draft code before Parliament.

238 Subsection (3) provides that, once the draft code of practice has been laid before Parliament, Parliament has 40 days within which it may resolve not to approve it. If either House of Parliament makes such a resolution, OFCOM must not issue the draft code and instead must prepare another version of it under clause 36.

239 If neither House of Parliament makes such a resolution, OFCOM must issue the code of practice and it will come into force after 21 days.

240 This clause applies in the same way to amendments to a code of practice as it does to a new code of practice, but not to minor amendments made under clause 43.

Clause 39: Secretary of State's powers of direction

241 Subsection (1) confers a power on the Secretary of State to direct OFCOM to modify a draft code of practice submitted to the Secretary of State under clause 38(1), if the Secretary of State believes that modifications are required for reasons of public policy or, in respect of the CSEA and terrorism codes only, for reasons of national security or public safety.

242 Subsection (2) qualifies this power by providing that, where the Secretary of State has required OFCOM to review a draft code of practice under clause 42(2), a direction may not be made under this clause requiring OFCOM to modify a draft code of practice unless the Secretary of State believes modifications are required for reasons of national security or public safety.

243 Subsection (3) allows the Secretary of State to direct OFCOM to modify a code of practice, following a review under clause 42(2) where OFCOM have decided no change is required and have submitted a statement to that effect under clause 42(3)(b), should the Secretary of State still believe that modifications are required for reasons of national security or public safety.

244 Subsection (4) requires that any direction to OFCOM under subsection (3) must be given within a period of 45 days from the day on which OFCOM's review statement is submitted to the Secretary of State, and must make particular reference to OFCOM's review statement.

245 Under subsection (5), a direction made under this clause cannot require OFCOM to include a particular step to be recommended to providers of regulated user-to-user or search services in a code of practice. The Secretary of State must give reasons for requiring modifications, except

where setting out those reasons would be against the interests of national security, public safety, or the relations with the government of a country outside the United Kingdom.

246 Subsection (6) provides that OFCOM must as soon as reasonably practicable comply with a direction made under this clause, and sets out what OFCOM must do when sending the modified draft code back to the Secretary of State.

247 Subsections (7) and (8) provide that the Secretary of State may direct OFCOM to make further modifications. Subsections (1) to (6) of this clause apply to any further directions.

248 Under subsection (9), once the Secretary of State is content that no further modifications are necessary, they must as soon as reasonably practicable lay the revised draft code of practice before Parliament, along with any document submitted by OFCOM that details what changes have been made to the draft code of practice, as mentioned in subsection (6)(c).

249 Subsection (10) allows the Secretary of State, with OFCOM's agreement, to remove or obscure information in OFCOM's review statement, prior to laying it before Parliament, where the Secretary of State considers that its disclosure would be against the interests of national security, public safety, or relations with the government of a country outside the United Kingdom.

250 Subsection (11) 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 38(1).

251 Subsection (12) defines "terrorism or CSEA code of practice" in this clause as a code of practice under clause 36(1) or (2).

Clause 40: Procedure for issuing codes of practice following direction under section 39

252 This clause explains the affirmative and negative procedures for parliamentary approval of the draft codes of practice and sets out when each of the procedures will be applied.

253 Subsection (1) sets out that this clause applies where a draft of a code of practice is laid before Parliament under clause 39(9).

254 Subsection (2) sets out that if the draft contains modifications made following a direction from the Secretary of State for reasons of public policy under clause 39(1)(a) then the affirmative procedure applies.

255 Subsection (3) sets out that if the draft terrorism or CSEA code of practice contains modifications made following a direction from the Secretary of State for reasons of national security or public safety under clause 39(1)(b), (2), or (3) then the negative procedure applies.

256 Subsection (4) sets out the affirmative procedure, which stipulates that a draft code of practice laid before Parliament under this procedure must not be issued by OFCOM unless the draft has been approved by each House of Parliament. If the draft is approved, then it comes into force 21 days from the day on which it was issued. If the draft is not approved, OFCOM must prepare another draft under clause 36.

257 Subsection (5) sets out the negative procedure, which stipulates that a code of practice laid before Parliament under this procedure will be issued by OFCOM after a 40 day period, unless Parliament resolves not to approve it. If Parliament resolves not to approve the draft codes then OFCOM must prepare another draft under clause 36.

258 Subsection (6) defines "40 day period" as having the same meaning as is in clause 38.

259 Subsection (7) sets out that this clause also applies to drafts of amendments of a code of practice laid before Parliament under clause 39(9).

Clause 41: Publication of codes of practice

260 This clause sets out what OFCOM must do once a code is ready for publication. Subsections (1) and (2) state that OFCOM must publish a code of practice or amendments to a code of practice within three days of the code or amendments being issued under clause 38 or 40.

261 Subsection (3) requires OFCOM to publish a notice where a code has been withdrawn.

Clause 42: Review of codes of practice

262 This clause makes provision for review of codes of practice by OFCOM. Subsection (1) requires OFCOM to keep all published codes of practice under review.

263 Subsection (2) gives the Secretary of State the power to require OFCOM to review a code of practice on terrorism or CSEA if the Secretary of State deems it necessary for reasons of national security or public safety; and requires the Secretary of State to notify OFCOM of which category the reasons fall into. OFCOM must then carry out a review and either prepare a draft of amendments to the code of practice if they consider that changes are required or, if not, submit a statement to the Secretary of State explaining the reasons for that conclusion.

264 OFCOM must publish the statement submitted to the Secretary of State as soon as is reasonably practicable after a period of 45 days has elapsed, if the Secretary of State has not given a direction to make modifications under clause 39(3).

265 Subsection (6) allows the Secretary of State to make representations to OFCOM regarding the removal or obscuring of information in the statement in the interests of national security, public safety, or relations with the government of a country outside the United Kingdom

Clause 43: Minor amendments of codes of practice

266 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.

Clause 44: Relationship between duties and codes of practice

267 This clause sets out how providers of Part 3 services can comply with their relevant duties under this Bill.

268 Subsection (1) states that providers will be treated as complying with their duties if they follow the recommended measures set out in the relevant codes of practice. Subsections (2)

and (3) provide that user-to-user service and search service providers are to be treated as complying with their duties to protect users' rights to freedom of expression and privacy if they follow the measures in the codes incorporating safeguards for the protection of freedom of expression and privacy. Separately, subsection (4) makes this provision for providers of Category 1 or Category 2A services in relation to a fraudulent advertising code.

269 A provider is not obliged to follow a code of practice; they may instead take alternative measures to comply with the relevant duties in the legislation.

270 Where a regulated provider seeks to comply with a relevant duty by taking alternative measures to those set out in the codes, they must have particular regard to protecting users' rights to freedom of expression and privacy (subsection (5)). When OFCOM assess compliance when a regulated provider has taken alternative measures to those set out in the codes of practice, they must also consider the extent to which users' rights have been safeguarded (where relevant) (subsection (6)).

Clause 45: Effects of codes of practice

271 Subsection (1) provides that not taking or using a measure in a code of practice does not of itself make the provider liable to legal proceedings.

272 Subsection (2) confirms that codes of practice can be used as evidence in legal proceedings. Subsection (3) requires a court or tribunal, when determining a question in legal proceedings, to take into account a provision of a code of practice that was in force at the time relating to the question and appears to the court to be relevant.

273 Subsection (4) puts an equivalent requirement on OFCOM when they determine a question which arises in connection with their exercise of a relevant function.

Clause 46: Duties and the first codes of practice

274 This clause establishes that duties in respect of which OFCOM must issue a code of practice (under clause 36) will only apply once the first code of practice for that duty has come into force. This could mean that different duties will apply at different times, depending on when the relevant code for a particular duty comes into force. This clause specifies the relevant duties and the corresponding codes under clause 36.

275 Clause 46(9) specifies that this clause is subject to Part 2 of Schedule 17. This is intended to clarify that a provider of a service currently regulated by Part 4B of the Communications Act 2003 does not need to comply with the safety duties while subject to the transitional arrangements set out in Part 2 of Schedule 17.

Guidance

Clause 47: OFCOM's guidance about certain duties in Part 3

276 Subsections (1) and (2) require OFCOM to produce guidance for providers of relevant services on how to carry out their record-keeping and review duties at clauses 19 and 29, the children's access assessment duties at clause 31 and (for providers of Category 1 services) the duties to protect news publisher content at clause 14.

277 Subsection (3) requires OFCOM to consult the Information Commissioner before preparing, revising or replacing guidance relating to the record-keeping and review duties at clauses 19 and 29, and the children's access assessment duties at clause 31.

278 OFCOM must publish the guidance produced, including any revised guidance (subsection (4)).

Clause 48: OFCOM's guidance: content that is harmful to children and user empowerment

279 Subsections (1) and (2) require OFCOM to produce guidance which contains examples of content that OFCOM considers to be (or not to be):

a. for providers of Part 3 services, primary priority and priority harmful content to children, and

b. for providers of Category 1 services, content to which the user empowerment duty in section 12(2) applies.

280 Subsection (3) requires OFCOM to consult with persons they consider appropriate before producing this guidance.

281 OFCOM must publish the guidance they produce, including any revised guidance (subsection (4)).

Chapter 7: Interpretation of Part 3

Clause 49: "Regulated user-generated content", "user-generated content", "news publisher content"

282 This clause defines "regulated user-generated content" and describes the types of user-generated content that are exempt from this definition, including "news publisher content". Part 3 duties on regulated user-to-user services apply to "regulated user-generated content".

283 Subsections (3) and (4) define "user-generated content". This is 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. This means that 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.

284 Subsection (5) defines "one-to-one live aural communications". It states that aural communications between two users which are not accompanied by written messages, videos or other visual images (other than identifying content, such as a user name or profile picture) and which are not recordings of such content, are exempt from the definition of "regulated user-generated content". For example, a one-to-one live voice call over an internet service would not count as "regulated user-generated content", but a one-to-one video call or a recording of a call shared on a regulated service would. This exemption is expressed as applying to "aural" communications, rather than just to "oral" communications, in order to

cover all audio communications (i.e. speech and other sounds), rather than simply speech. This ensures that one-to-one calls akin to traditional telephony are not in scope.

285 Subsections (6) and (7) define "comments and reviews on provider content" in respect of user-to-user services. This definition encompasses user comments and reviews in relation to all content that is published on a service by the service provider or someone acting on their behalf. These are excluded from the definition of "regulated user-generated content", meaning that user-to-user services have no duties with regard to them. In practice, this means that comments and reviews on recognised news publishers' sites and on many sites selling goods and services are not in scope of the regulatory framework. This exemption does not exclude comments or reviews on user-generated content, such as content posted by third party sellers offering goods or services on online marketplaces.

286 Subsections (8) to (10) define "news publisher content". This includes any content on a service directly generated by a recognised news publisher (as defined in clause 50). In addition, it includes content originally published by a recognised news publisher but uploaded to or shared on a service by a user of that service, either in its entirety or by way of a link to the entirety of the material. 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 a user amends content generated by a recognised news publisher that content will count as user-generated content, as will any user-generated text or images accompanying the news publisher content.

Clause 50: "Recognised news publisher"

287 This clause defines the term "recognised news publisher". Subsection (1)(a) to (c) states that the British Broadcasting Corporation, Sianel Pedwar Cymru, and any entity that holds a licence under the Broadcasting Act 1990 or 1996 and which publishes news-related content under that licence will qualify as a recognised news publisher.

288 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).

289 Subsection (3) sets out the conditions in which an entity is excluded from the definition of "recognised news publisher" 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.

290 Subsection (4)(a) 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).

Clause 51: "Search content", "search results" etc

291 This clause defines "search content" and describes the types of content that are exempt from this definition, including paid-for advertisements and content on the website of a recognised news publisher.

292 "Search content" is content that may be encountered in or via search results of a search service or search engine. Search results are the content which is presented to a user of the service by the search engine when they make a search request. Typical examples would be a link to a website or an image on an image search results page. Search results may also include short pieces of text from a website, media in other forms, links which are icons or anything else provided it is presented by the operation of the search engine when a search request is made.

293 Content encountered "via search results" is content which is presented to a user when they interact with a search result itself, for example by clicking on it. It does not include content which a user comes across as a result of any subsequent interaction (that is, interaction with anything other than a search result). This means that search content includes content on a webpage that can be accessed by interacting with search results.

294 "Search" is widely defined to capture the variety of different ways in which search engines can be operated, including speech-based virtual assistants.

Clause 52: Restricting users' access to content

295 This clause clarifies the meaning of the expression "restricting users' access to content" for the purposes of Part 3 of the Bill, including in relation to the content of democratic importance, journalistic content and news publisher protections (clauses 13 to 15). The expression is also used in Part 4 of the Bill, in the transparency, accountability and freedom of expression duties (clauses 64 and 65), where it has the same meaning as here (see clause 67(4)).

296 Subsection (2) makes clear that the expression covers cases where a provider prevents a user from accessing content without that user taking a prior step (such as clicking past a warning notice), or where content is temporarily hidden from a user.

297 Subsection (3) makes clear that this expression does not cover any restrictions the provider puts in place to enable users to apply user-empowerment tools to limit the content that they encounter, or cases where access to content is controlled by another user rather than by the provider (for example, where users have the power to take moderation decisions in private or semi-private spaces on the service).

Clause 53: "Illegal content" etc

298 This clause defines "illegal content" as content which amounts to a relevant offence (subsections (2) and (3)).

299 Subsection (4) defines a "relevant offence" as a priority offence (defined in subsection (7) as an offence specified in Schedule 5, 6 or 7) or an offence within subsection (5).

300 Subsection (5) covers any offence which is not a priority offence, which has an individual victim or intended victim, and which is created by an Act of Parliament or by certain other specified kinds of legislation. Subsection (6) excludes certain types of offences from the definition of "relevant offence".

301 Subsection (10) defines priority illegal content as terrorism content, CSEA content or content that amounts to an offence listed in Schedule 7. "Terrorism content" and "CSEA content" are defined in subsections (8) and (9) respectively.

302 Under subsection (11), content does not need to be generated, uploaded or accessed (or have anything else done in relation to it) in any part of the United Kingdom to amount to an offence under this provision. This is the case regardless of whether the criminal law would require any relevant action to take place in the United Kingdom (or a particular part of it).

303 Subsection (12) ensures that content generated by a bot is capable of being illegal content.

304 Subsections (13) and (14) clarify that for user-to-user services and the user-to-user part only of combined services, 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 these definitions because it had not yet been uploaded to or shared on a service.

305 Content amounting to any offence under the law of England and Wales, Scotland or Northern Ireland which meets the definition under subsection (4) is illegal content (including, as appropriate, priority illegal content) in all parts of the United Kingdom for the purposes of the Bill.

Schedule 5: Terrorism offences

306 Schedule 5 sets out the offences that constitute "terrorism offences". These are offences contained 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 terrorism offences.

307 Paragraph 1 lists the relevant provisions that apply from the Terrorism Act 2000.

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

309 Paragraph 3 lists the relevant provisions that apply from the Terrorism Act 2006.

310 Paragraph 4 sets out the offences that constitute an inchoate offence. These offences include attempting or conspiring to commit an offence in the Schedule, or encouraging or assisting, aiding, abetting, counselling or procuring the commission of one of those offences (or in Scotland being involved in the commission of such an offence).

Schedule 6: Child sexual exploitation and abuse offences

311 Schedule 6 sets out the offences, in the component jurisdictions of the United Kingdom, that constitute "CSEA offences". The Bill does not introduce any new CSEA offences.

312 Schedule 6, Part 1 lists the relevant CSEA offences in England, Wales and Northern Ireland.

313 Paragraph 1 sets out the offence under the Obscene Publications Act 1959, relating to an obscene article tending to deprave and corrupt others. The inclusion of this offence is for

instances in which the article would encourage an individual to commit a CSEA-related offence listed in paragraphs 2, 4, 5, 7 or 8.

314 Paragraph 2 sets out offences with regard to indecent photographs, and pseudo-photographs of children: taking; permitting to be taken; making, distributing or showing, possessing with a view to their being distributed or shown by himself or others; and publishing, or causing to be published, any advertisement likely to be understood as conveying that the advertiser distributes or shows such indecent photographs.

315 Paragraph 3 sets out equivalent offences in Northern Ireland regarding indecent photographs, or pseudo-photographs, of children, as set out in the Protection of Children (Northern Ireland) Order 1978.

316 Paragraph 4 lists the offence of possession of any indecent photograph, or pseudo-photograph of a child, as set out in Section 160 of the Criminal Justice Act 1988.

317 Paragraph 5 lists relevant CSEA-related offences from the Sexual Offences Act 2003 which can be committed online.

318 Paragraph 6 lists equivalent relevant CSEA-related offences in Northern Ireland from the Sexual Offences (Northern Ireland) Order 2008.

319 Paragraph 7 lists the offence under Section 62 of the Coroners and Justice Act 2009 (possession of a prohibited image of a child).

320 Paragraph 8 lists the offence under section 69 of the Serious Crime Act 2015 (possession of paedophile manual).

321 Paragraph 9 lists CSEA-related inchoate offences: the offence of attempting or conspiring to commit an offence specified in this Part (Schedule 6, Part 1); an offence under Part 2 of the Serious Crime Act 2007 (encouraging or assisting) in relation to an offence specified in this Part; and an offence of aiding, abetting, counselling or procuring the commission of an offence specified in this Part.

322 Schedule 6, Part 2 lists the relevant CSEA offences in Scotland. Paragraph 10 sets out the relevant offences under the Civic Government (Scotland) Act 1982: section 52 (indecent photographs etc of children) and section 52A (possession of indecent photographs of children).

323 Paragraph 11 lists relevant CSEA offences from the Protection of Children and Prevention of Sexual Offences (Scotland) Act 2005.

324 Paragraph 12 lists relevant CSEA offences from the Sexual Offences (Scotland) Act 2009.

325 Paragraph 13 lists CSEA-related inchoate offences: attempting or conspiring to commit an offence specified in this Part; inciting a person to commit an offence specified in this Part; and aiding, abetting, counselling or procuring the commission of an offence specified in this Part, or being involved art and part in the commission of such an offence.

Schedule 7: Priority offences

326 Content which amounts to the criminal offences which are listed in Schedules 5, 6 and 7 is priority illegal content. Terrorism and CSEA offences are set out in Schedules 5 and 6 respectively. Schedule 7 lists the other priority offences. Paragraph 4 of Schedule 5, paragraphs 9 and 13 of Schedule 6, and paragraph 33 of Schedule 7 also set out the inchoate offences that constitute priority offences. These include attempting or conspiring to commit an offence in the Schedule, or encouraging or assisting, aiding, abetting, counselling or procuring the commission of one of those offences (or in Scotland being involved in the commission of such an offence).

327 The National Security Bill has been amended so as to make the foreign interference offence a priority offence for the purposes of this legislation once that offence has been brought into law.

Clause 54: "Content that is harmful to children" etc

328 This clause defines "content that is harmful to children".

329 Subsections (2) and (3) define "primary priority content that is harmful to children" and "priority content that is harmful to children". These are descriptions of content which the Secretary of State has designated in regulations (see clause 55).

330 Subsection (4) defines "content that is harmful to children" as primary priority or priority content that is harmful to children or a third category of "non-designated content that is harmful to children" - another kind of content which presents a material risk of significant harm to an appreciable number of children in the United Kingdom.

331 The references to content that presents "a material risk of significant harm to an appreciable number of children in the United Kingdom" in the criteria for the designation of descriptions of primary priority and priority content and in the definition of "non-designated content that is harmful to children" means that content need not adversely affect a very large number of children to be classified as harmful to children, but content which may adversely affect only one child or very few children will not be caught by the definition of "content that is harmful to children". "Harm" is itself defined in clause 205.

332 Subsection (5) excludes certain types of content from the definition of "content that is harmful to children". These types of content are illegal content (which is dealt with separately by other provisions in the Bill) and content where the risk of harm comes from the content's potential financial impact, the safety or quality of goods featured in the content or a way in which a service featured in the content may be performed.

Clause 55: Regulations under section 54

333 This clause makes provision in relation to the making of regulations under clause 54 designating primary priority and priority content that is harmful to children. The Secretary of State may only specify a description of content in regulations if the Secretary of State considers that there is a material risk of significant harm to an appreciable number of children in the

United Kingdom presented by regulated user-generated or search content of that description, and must consult OFCOM before making such regulations.

Clause 56: Regulations under section 54: OFCOM's review and report

334 This clause imposes a duty on OFCOM to carry out reviews of the prevalence and severity of content that is harmful to children on regulated user-to-user services and search services. It requires OFCOM to prepare and publish reports on the outcomes of each review at least every three years, and include in those reports advice as to whether it is appropriate for the Secretary of State to make changes to the regulations made under clause 54 setting out primary priority and priority content that is harmful to children.

Part 4: Other duties of providers of regulated user-to-user services and regulated search services

Chapter 1: User identity verification

Clause 57: User identity verification

335 This clause places a duty on all providers of Category 1 services to offer adult users the option to verify their identity. Providers will have discretion as to which form of identity verification they offer.

336 Providers must make it clear to users in their terms of service what form of identity verification is available and how the verification process works.

Clause 58: OFCOM's guidance about user identity verification

337 This clause places a requirement on OFCOM to produce and publish guidance for providers of Category 1 services to assist them in complying with the user identity verification duty in clause 57(1).

338 As part of preparing the guidance, OFCOM must have particular regard to the desirability of ensuring that the recommended identity verification measures are accessible to vulnerable users. In preparing the guidance OFCOM must consult the Information Commissioner, persons with relevant technical expertise, persons representing the interests of vulnerable adult users and anyone else they consider appropriate.

Chapter 2: Reporting Child Sexual Exploitation and Abuse Content

Clause 59: Requirement to report CSEA content to the NCA

339 This clause sets out the requirement on relevant services to report CSEA content to the National Crime Agency (NCA). The NCA will be the organisation responsible for receiving reports from services via secure transmission, processing reports including triaging and disseminating reports to law enforcement and other appropriate agencies in the United Kingdom and internationally.

340 Subsection (1) states that a UK provider of a regulated user-to-user service must have systems and processes in place which are capable of making all detected and unreported CSEA content into a report and that these reports are submitted to the NCA.

341 Subsection (2) places the same requirement on non-UK providers of regulated user-to-user services. Non-UK services will only be required to report CSEA content to the NCA where they can establish a UK link, unless that provider is already reporting all CSEA content, including UK-linked CSEA content to overseas law enforcement or an alternative reporting body outside the UK – whether on a mandatory or voluntary basis.

342 It is a service's responsibility to ensure all relevant UK offences are reported to the NCA or reported to another body under an alternative reporting regime, regardless of whether the content constitutes an offence in the country the service is based. If the service starts to voluntarily report these additional offences to the relevant reporting body in their country they will remain exempt from this requirement.

343 Subsection (3) sets out the reporting requirement for UK providers of regulated search services. Search services will be required to report CSEA content which they detect during routine web crawling which those services already carry out for business purposes. This element of the reporting duty is separate from safety duties under the Bill.

344 Subsection (4) places the same requirement on non-UK providers of regulated search services where there exists a UK link to the CSEA content.

345 Subsection (7) sets out that reports must meet requirements set out in regulations and must be sent to the NCA in the manner, and within timeframes set out in regulations.

346 Subsection (10) states that the requirement to report CSEA content will be based on when it is detected, not when the offence occurred. An offence may have occurred before the commencement of this requirement, but if it is detected on or after commencement, the service would need to report it.

Clause 60: Regulations about reports to the NCA

347 This clause places a duty on the Secretary of State to produce regulations about the reports being made to the NCA.

348 Subsection (2) lists the provisions which may be covered in regulations but is not exhaustive. The information that can or should be reported will vary depending on the nature of the service and the offence that has occurred. Services will be required to report all and any available information relating to instances of CSEA, including any that help identify a perpetrator or victim.

349 Services will need to include information relating to the identity of any individual who is suspected of committing a CSEA offence; information relating to the geographic location of the involved individual or website, which may include the Internet Protocol address or verified address; evidence of the CSEA offence itself, such as indecent images or sexual communications between an adult and a child; and any information relating to a child.

350 Subsection (3) requires that before making (including revising), regulations, the Secretary of State must consult the NCA, OFCOM and any other appropriate persons. Regulations will be adaptable to allow for ongoing technological and industry developments and can be revised as necessary.

Clause 61: NCA: information sharing

351 This clause amends the definition of "permitted purpose" in section 16(1) of the Crime and Courts Act 2013 to allow the NCA to disclose information to OFCOM for the purpose of its functions under this legislation.

Clause 62: Offence in relation to CSEA reporting

352 This clause sets out the offence of providing false information in relation to the reporting requirement.

353 Subsection (1) states that an offence has been committed where a person provides false information either knowingly or without regard to its accuracy.

354 Subsections (2) sets out the sentencing for a person who is convicted of this offence in England and Wales, Scotland and Northern Ireland.

Clause 63: Interpretation of this Chapter

355 This clause provides clarification of terms used in this chapter.

356 Subsection (4) provides clarification of when content is considered "detected". This content may be detected by the service provider through a number of means, including automated monitoring systems (such as hash matching), human moderators or user reports. The requirement to report CSEA content will be based on when content is detected, not when the offence occurred.

357 Subsection (5) sets out that content is considered "'unreported" by the service if that service does not meet exemptions listed at subsection (5)(a) and (5)(b) by reporting on to a foreign agency or to the NCA. The reporting to the foreign agency may be on a mandatory or voluntary basis.

358 Subsection (6) describes the term "UK-linked" for the purpose of the reporting requirement. The content may be UK-linked based on the place where content is published, generated, uploaded or shared in the United Kingdom; the nationality of the person suspected of committing the related offence; or where the person suspected of committing the related offence is located in the United Kingdom or where the child who is the suspected victim of the related offence is located in the United Kingdom. Where a non-United Kingdom service is able to establish a United Kingdom link as described in subsection (6), this content must be reported to the NCA if it has not already been reported under alternative voluntary or mandatory reporting regimes. The information that a service provider has available to them to determine whether CSEA content is linked to the United Kingdom will vary depending on the nature of that service and the information they collect on their users. The legislation does not specify how services could determine location, but this can be determined through multiple

indicators, which may include IP addresses, Media Access Control (MAC) addresses, information provided by users on their profiles, etc.

359 There will not be a consequence if the provider reports CSEA content to the NCA which the provider thinks might have a link to the United Kingdom, but does not.

360 The term "foreign agency" noted at subsection (7) denotes the exemption for services who report under alternative voluntary or mandatory reporting outside of the United Kingdom.

Chapter 3: Terms of service: Transparency, accountability, and freedom of expression

Clause 64: Duty not to act against users except in accordance with terms of service

361 This clause ensures Category 1 service providers only remove or restrict access to content, or ban or suspend users, where this is consistent with their terms of service or where they face another legal obligation to do so.

362 Subsection (1) sets out the duty on Category 1 service providers to have systems and processes designed to ensure they only remove or restrict access to content, or ban or suspend users, where this is consistent with their terms of service.

363 Subsection (2) provides that the duty in subsection (1) does not apply to actions taken as a result of providers' compliance with their illegal content duties and child safety duties. Actions taken to avoid criminal or civil liability are also exempt from the duty in subsection (1).

364 Subsection (3) sets out that the duty in subsection (1) also does not apply to the removal or restriction of access to content that constitutes an offence, or against a user who has uploaded, generated or shared content that constitutes an offence. Subsection (1) also does not apply where a service bans or suspends a user responsible for or involved in placing fraudulent advertisements on their service. Subsection (7) defines "offence" and "fraudulent advertisement"' for the purposes of this clause. It also defines "criminal or civil liability".

365 Subsection (4) exempts consumer content and terms of service about such content from the duty in subsection (1). Clause 67(3) has the effect of defining consumer content as (a) all regulated user-generated content that is directly connected with the sale of goods or supply of services by consumers and traders who are users of a service, (b) all regulated user-generated content that amounts to an offence under the Consumer Protection from Unfair Trading Regulations 2008, and (c) any other regulated user-generated content that is covered by those Regulations. Such content is already regulated by the Competition and Markets Authority and other consumer protection bodies. The exclusion avoids regulatory overlap between OFCOM and those bodies, and ensures that the duties in this clause do not inadvertently create a barrier for the enforcement of consumer protection legislation.

Clause 65: Further duties about terms of service

366 This clause imposes further duties about terms of service on regulated user-to-user service providers and Category 1 service providers.

367 Subsection (1) requires all providers of regulated user-to-user services to include a provision in their terms of service informing users about their right to bring a claim in court for breach of contract where their content, or their account, is removed, restricted or suspended in breach of the terms of service. This seeks to increase transparency about users' existing legal rights; it does not create a new right of action.

368 Subsection (3) requires Category 1 service providers to put in place systems and processes to enforce any terms of service that they set relating to the removal or restriction of legal content, and the banning or suspension of users.

369 Subsection (4) requires that such terms of service are clear and accessible. These terms must be easy for users to understand and be written with sufficient detail so users know what to expect in relation to moderation actions taken by the provider. Providers of Category 1 services must also apply their terms of service consistently such that moderation decisions are made in the same way for similar pieces of content.

370 Subsections (5)-(8) require Category 1 service providers to ensure their users can report any content or accounts that the user deems to violate the service's terms of service, and to make complaints about providers' moderation actions and compliance with their duties under this clause. Providers are required to take appropriate action in response to complaints. The complaints procedure must be easy to use, easy to access, transparent, and specified in terms of service.

371 Subsection (9) excludes terms of service in relation to the illegal content and child safety duties from the duties in this clause, as well as terms of service about consumer content. Consumer content is defined in clause 67(3), and related terms of service are exempt from these duties because they are already regulated by the Competition and Markets Authority and other consumer protection bodies.

Clause 66: OFCOM's guidance about duties set out in sections 64 and 65

372 This clause requires OFCOM to produce and publish guidance for Category 1 service providers to help them comply with their duties in clauses 64 and 65(3) to (7).

Clause 67: Interpretation of this Chapter

373 This clause clarifies terms used in clauses 64 and 65.

374 Subsection (2) sets out that 'regulated user-generated content' has the same meaning as in Part 3 of the Bill.

375 Subsection (3) defines 'consumer content' for the purposes of clauses 64(4) and 65(9).

376 Subsection (4) provides that references to 'restricting users' access to content' in this Chapter are to be understood in accordance with clauses 52 and 207(5).

377 Subsection (5) sets out the definition of 'relevant content' for the purposes of clause 65(5) and (8). This covers regulated user-generated content that a term of service (other than one relating to the illegal content and child safety duties, or consumer content) states that a provider may or will take down or restrict users' access to.

378 Subsection (6) sets out the meaning of an 'affected person' for the purposes of the user redress provisions in clause 65(8).

379 Subsection (7) sets out that the size and capacity of a Category 1 service provider are particularly relevant when deciding what steps are proportionate for a service provider to take to comply with its duties under clauses 64 and 65.

Chapter 4: Transparency Reporting

Clause 68: Transparency reports about certain Part 3 Services

380 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 is intended to help users understand the steps providers are taking to keep them safe, and to provide OFCOM with the information required to hold them to account.

381 Transparency reports are required from Category 1, Category 2A and Category 2B services, as included in the register of categories of certain Part 3 Services (established under clause 86). OFCOM may request different types of information depending on which category a particular service meets the conditions for. The Secretary of State may change by regulations the frequency of production of transparency reports, and must consult OFCOM before doing so.

Schedule 8: Transparency reports by providers of Category 1 services, Category 2A services and Category 2B services

382 Schedule 8 lists matters about which information may be required from Category 1 and Category 2B services (Part 1) and Category 2A services (Part 2) in their transparency reports under clause 68. It describes high-level types of information that OFCOM will be able to require a service provider to report on. OFCOM will then set out the specific information within these categories that service providers will need to report on in a notice. This will give OFCOM the flexibility to tailor the reporting requirements so the information sought is as useful as possible. It will also allow OFCOM to account for differences between services in setting the transparency requirements and will allow the requirements to evolve over time.

383 This schedule also sets out various factors that OFCOM must take into account when deciding which types of information to require under clause 68. These include the service provider's capacity, the type of service and the functionalities the service offers, the number of users of the service and the proportion of users who are children. This will help ensure that the reporting requirements account for the differences between services and are proportionate. These factors are designed to help ensure the information that OFCOM selects is the most appropriate and proportionate type of information to require from the service provider in question.

Clause 69: OFCOM's guidance about transparency reports

384 This clause places a requirement on OFCOM to prepare and publish guidance on how they will exercise their power relating to transparency reports. Subsection (1) sets out the matters which must be included in guidance and subsection (2) lists expert bodies and interested parties which must be consulted before preparing this guidance, if OFCOM consider them

appropriate consultees. OFCOM must have regard to this guidance when preparing or giving a notice to a provider to produce a transparency report (under clause 68) or producing their own transparency reports (under clause 145).

Part 5: Duties of providers of regulated services: Certain pornographic content

Clause 70: "Pornographic content", "provider pornographic content" "regulated provider pornographic content"

385 This clause sets out what content the duties in clause 72 apply to.

386 Subsection (2) defines what content (see clause 207 for the definition of content) is considered to be pornographic for the purposes of Part 5.

387 Subsection (3) sets out what is meant by "provider pornographic content". This is pornographic content which is published or displayed on a service by the service provider itself, or an individual acting on behalf of the service provider. It does not include user-generated content (as set out in subsection (6)). Provider pornographic content also includes pornographic content which is published or displayed on the service by means of software, automated tools, or algorithms. This may include instances where the provider displays on the service thumbnails of images or videos which are hosted on the server of a third party.

388 Subsection (4) sets out that "regulated provider pornographic content" is any content which meets the definition of "provider pornographic content" but does not include text-only content or paid-for advertisements (see clause 207 for the definition of paid-for advertisement).

389 Subsection (5) clarifies that pornographic content that is "published or displayed" on a service includes content that may require user interaction in order to be visible or audible (for example, by clicking on content that is blurred, distorted, or obscured) if that content is present on the service but not such content that is in the search results of a search service or a combined service. It clarifies that pornographic content that is "published or displayed" on a service includes content that is embedded on the service.

390 Subsection (6) provides that user-generated content, as defined in clause 49 is not to be considered provider pornographic content for the purposes of subsection (3). This subsection keeps the categories of user-generated content and provider pornographic content mutually exclusive.

Clause 71: Scope of duties about regulated provider pornographic content

391 Subsections (1) and (2) set out the providers of internet services which are required to comply with the duties under clause 72. Providers are required to comply i) where they have regulated provider pornographic content published or displayed on their service, ii) they are not exempt as set out in subsection (3), and iii) have links with the United Kingdom for the purposes of this Part as set out in subsection (4).

392 Subsection (3) sets out that a service is exempt if it is a user-to-user or search service that is exempt as provided for by Schedule 1 or any internet service described in Schedule 9. A service which is exempt from the Part 3 duties by virtue of Schedule 2 is not exempt from the duties in clause 72 unless the service is also a service described in Schedule 9. An example of a type of service which is exempt from Part 3 but in scope of Part 5 is a limited functionality service (for example a service whose only user-to-user functionality is users posting comments about provider content) which publishes regulated provider pornographic content.

393 Subsection (4) sets out that a service "has links to the United Kingdom" if it has a significant number of users in the United Kingdom or if the service is targeted partially or solely at users in the United Kingdom.

394 Subsection (5) states that Part 5 does not apply to a part of a regulated service if that part meets the definition of an internal business service in either: (a) paragraph 7(2) of Schedule 1 if it is a Part 3 service, or (b) in paragraph 1(2) of Schedule 9 if it is an internet service which is not a Part 3 service. Part 5 may still apply to the non-internal business service part of the service if that part has regulated provider pornographic content. Further exemptions for internal business services are contained in Schedule 9.

395 The effect of subsection (6) is that the duties of Part 5 do not apply to the part of a regulated service which is an on-demand programme service (ODPS) as defined by section 368A of the Communications Act 2003. Part 5 may still apply to the non-ODPS part of the service if that part has regulated provider pornographic content. Further exemptions for ODPS are contained in Schedule 9.

396 The purpose of the combination of exemptions contained in subsections (5), (6), and paragraphs 2 and 6 of Schedule 9 is to provide for where only part of a service is exempt and the remainder of the service remains in scope of Part 5.

397 Subsection (8) clarifies that a service provider's compliance with the duties in clause 72 only applies to the design, operation and use of the service in the United Kingdom or as it affects United Kingdom users of the service.

Schedule 9: Certain internet services not subject to duties relating to regulated provider pornographic content

398 Schedule 9 sets out the providers of internet services which are not subject to the duties on regulated provider pornographic content.

399 This includes services which meet the definition of internal business services (either as a whole or for part of the service) and which are not user-to-user or search services. It also includes services provided by public bodies or services provided for by persons providing education or childcare. It also includes internet services which are an on-demand programme service as defined by section 368A of the Communications Act 2003 (either as a whole or for part of the service). Clause 71(6) also makes provision for when on-demand programme services are not subject to the duties in clause 72.

Clause 72: Duties about regulated provider pornographic content

400 Clause 72 establishes the duties which apply to providers of services with regulated provider pornographic content as set out in clause 71(2).

401 Subsection (2) requires service providers to restrict those under the age of 18 from being able to view regulated provider pornographic content on their service. Service providers will most likely need to use age verification to comply with these duties. Age verification refers to the age assurance measures that provide the highest level of confidence about a user's age.

402 Subsection (3)(a) requires service providers to keep an easily understood, written record of the measures they have taken or which are in use, and any policies they have implemented, to comply with the duty in subsection (2). Subsection (3)(b) requires service providers to keep such a record of the ways they have protected users from a breach of any statutory provision or rule of law concerning privacy (including, but not limited to, any such provision or rule concerning the processing of personal data).

Clause 73: OFCOM's guidance about duties set out in section 72

403 This clause requires OFCOM to produce guidance for providers of services with regulated provider pornographic content as set out in clause 71(2) to assist them in complying with the duties under clause 72.

404 Subsection (2) sets out what OFCOM must include within guidance under this section. The intention is that the guidance will provide services with practical examples to assist them with complying with their obligations which are set in primary legislation. The guidance will also provide additional transparency on how OFCOM will determine if a service has complied with its duties under clause 72.

405 Subsection (3) requires OFCOM to consult with particular persons as set out in this subsection prior to preparing, revising, or replacing the guidance for providers.

406 Subsection (4) provides that where OFCOM consider any proposed changes to the guidance to be of a minor nature, there is no requirement on OFCOM to consult as set out subsection (3) providing the Secretary of State is notified of the proposed changes and agrees that the amendments are minor and consultation is unnecessary.

407 Subsection (5) places a duty on OFCOM to keep the guidance under this section under review. Subsection (6) places a duty on OFCOM to publish the guidance and any revised or replacement guidance produced under this section.

Part 6: Duties of providers of regulated services: fees

Clause 74: Duty to notify OFCOM

408 The cost to OFCOM of exercising their online safety functions will be met by fees charged to providers of regulated services. The regulated providers whose qualifying worldwide revenue is at or above a specified threshold must notify OFCOM for the relevant charging year as per the conditions set out in clause 74(1)(a) and (1)(b). A provider is not required to notify

OFCOM should they fall within an exemption designated by OFCOM and approved by the Secretary of State.

409 When notifying OFCOM, regulated services must provide specific evidence within the timeframes stipulated in subsection (5).

410 The evidence which services must provide at the point of notification will be set out in regulations to be made by the Secretary of State. OFCOM will also issue a statement defining the terms "qualifying worldwide revenue" and "qualifying period".

Clause 75: Duty to pay fees

411 The cost to OFCOM of exercising their online safety functions will be met by fees charged to providers of regulated services. This clause empowers OFCOM to require a provider of a regulated service to pay the fee.

412 The fee payable to OFCOM will be based on the provider's qualifying worldwide revenue for the qualifying period and any other factors that OFCOM consider appropriate.

Clause 76: OFCOM's statement about "qualifying worldwide revenue" etc

413 This clause sets out the content of the statement, and the process to be followed, when OFCOM prepares the statement setting out the definition of "qualifying worldwide revenue" and "qualifying period".

414 Before publishing the statement, OFCOM must consult with the Secretary of State, the HM Treasury, and any other persons who OFCOM consider may be affected by the content in the statement.

415 OFCOM will publish and send a copy of the statement to the Secretary of State who will lay it before Parliament.

Clause 77: Threshold figure

416 OFCOM will be funded via fees from providers of regulated services whose qualifying worldwide revenue is equal to or greater than the specified threshold as determined by clause 77.

417 This clause sets out that OFCOM will consult persons affected by the threshold in order to inform the threshold figure for the purposes of clauses 74 and 75. The Secretary of State will then determine the figure for the threshold after having taken advice from OFCOM following the conclusion of the consultation.

418 Subsections (3)-(5) set out the process to be followed when the threshold is first set and each time it is revised.

Clause 78: Secretary of State's guidance about fees

419 This clause sets out the requirement for the Secretary of State to issue guidance to OFCOM regarding the principles to be included in their Statement of Principles (see clause 79).

420 The Secretary of State must consult with OFCOM before issuing or revising the guidance. The Secretary of State must also publish and lay the guidance (and any subsequent revisions)

before Parliament. OFCOM are required to have regard to the fees guidance when exercising their funding functions.

Clause 79: OFCOM's fees statements

421 The cost to OFCOM of exercising their online safety functions will be met by fees charged to providers of regulated services. OFCOM are required to produce a Statement of Principles that it will apply when setting the fees payable by providers of regulated services. Without publication of this document, OFCOM is not permitted to require providers to pay a fee.

422 The principles included in the Statement of Principles should justify that the fees payable are sufficient to cover OFCOM's operating costs and are justifiable and proportionate.

423 The content within the Statement of Principles must include the following: (a) details of the computation model used to calculate the fees; (b) the definition of qualifying worldwide revenue and qualifying period; and (c) the details of the threshold figure.

424 Subsection 9 (a) and (b) of this clause clarify that "OFCOM's costs" include costs incurred by OFCOM in preparing to carry out their online safety functions during a charging year and also include preparatory costs incurred after Part 6 of the Bill comes into force.

Clause 80: Recovery of OFCOM's initial costs

425 This clause introduces Schedule 10. The provisions in Part 6 of the Bill permit OFCOM to recover the costs set out at clause 79(9), incurred after the commencement of section 79, including the costs of preparations for the exercise of online safety functions as well as the costs of the actual exercise of online safety functions during a charging year.

426 Schedule 10 provides a mechanism whereby the costs incurred by OFCOM in undertaking work which directly or indirectly prepares OFCOM for their future role as the online safety regulator prior to the commencement of clause 79 of the Bill can be recovered by way of fees charged to providers of regulated services. In accordance with section 401(1) of the Communications Act and OFCOM's statement under that section, OFCOM have retained Wireless Telegraphy Act receipts to meet these costs.

427 Schedule 10 allows OFCOM to recover, from providers of regulated services, an amount equivalent to the amount of Wireless Telegraphy Act receipts OFCOM have retained to meet the costs incurred on preparations for the exercise of their online safety functions before the day on which clause 79 comes into force.

Schedule 10: Recovery of OFCOM's initial costs

428 This Schedule requires OFCOM to seek to recover their 'initial costs', which are costs incurred by OFCOM in undertaking work which directly or indirectly prepares OFCOM for their future role as the online safety regulator, before clause 79 comes into force by charging 'additional fees' to providers of services.

429 Paragraph 1 sets this out and makes it clear that the amount to be recovered is the amount of Wireless Telegraphy Act (WTA) receipts retained by OFCOM to meet those costs. The first phase of this process is set out in paragraph 2. OFCOM will charge additional fees over a

number of years, beginning after the initial charging year. The aggregate of those fees will equal the total of OFCOM's initial costs. Paragraph 7(5) sets out that that period will be no less than 3 and no more than 5 years.

430 Once that phase has been completed, there will be a second phase, as set out in paragraph 3. In the first year of this second phase OFCOM will charge fees to recover the outstanding amount, which is the amount of the additional fees yet to be recovered, which OFCOM consider are not likely to be paid or recovered, less any amount specified by the Secretary of State under paragraph 3(5). This process is repeated if necessary until all the money is either recovered, or OFCOM consider it is likely to be recovered, or the Secretary of State makes a determination under paragraph 4(2) that it does not need to be recovered. Paragraph 5 enables OFCOM to refund part of a fee where a provider is only a regulated service for part of a year.

431 Under paragraph 7 the Secretary of State must make regulations providing details of the additional fees, including the initial costs, the charging years, and the computation model. Before doing so they must consult OFCOM and providers in scope.

Clause 81: Meaning of "charging year" and "initial charging year"

432 This clause sets out the definitions of ''charging year'' and ''initial charging year''. The charging year will run for 12 months beginning on 1st April.

Part 7: OFCOM's powers and duties in relation to regulated services

Chapter 1: General Duties

Clause 82: General duties of OFCOM under section 3 of the Communications Act

433 This clause amends OFCOM's existing general duties under section 3 of the Communications Act 2003 (CA 2003), in order to set out duties applicable to OFCOM's new role as the online safety regulator.

434 This clause introduces a new general duty on OFCOM to secure, in the carrying out of their functions, the adequate protection of citizens from harm arising from content on regulated services, through the appropriate use by providers of such services of systems and processes designed to reduce the risk of such harm.

435 The amendments include listing the factors that OFCOM must have regard to in performing the new general duty, and specifying that OFCOM do not need to have regard to the desirability of promoting and facilitating the development of self-regulation in carrying out their functions under the Online Safety Act 2023.

436 This clause also provides that the terms 'content', 'harm', 'provider', and 'regulated service' have the same meaning in the CA 2003 as in the Online Safety Act 2023.

Clause 83: Duties in relation to strategic priorities

437 This clause sets out OFCOM's duties in relation to statements of strategic priorities designated by the Secretary of State under clause 153(1).

438 In particular, OFCOM must have regard to any such statement in carrying out their online safety functions.

Clause 84: Duty to carry out impact assessments

439 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 their online safety functions.

440 Section 7(2A) of the CA 2003 will provide that all proposals to introduce, replace or amend codes of practice under the Online Safety Act 2023 are "important proposals" for the purposes of OFCOM's duty to carry out impact assessments. This means that OFCOM will 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.

441 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 regulated user-to-user services and regulated search services

Clause 85: Meaning of threshold conditions etc

442 This clause sets out how Schedule 11, which provides details about the regulations for establishing threshold conditions, applies in relation to Part 3 Services.

Schedule 11: Categories of regulated user-to-user services and regulated search services: regulations

443 This Schedule sets out the procedure for making and amending the regulations that establish the threshold conditions a relevant service must meet in order to be designated as a Category 1, Category 2A or Category 2B service.

444 Paragraphs 1(1) and (3) state the Secretary of State must make regulations specifying threshold conditions for Category 1 and 2B relating to number of users, functionalities, and any other relevant characteristics and factors. Paragraph 1(2) states the regulations for Category 2A threshold conditions must relate to number of users, and any other relevant characteristics and factors.

445 Paragraph 1(4) provides that these regulations must specify how a service may meet the relevant threshold conditions. It makes clear that, in order to meet the threshold conditions to become a Category 1 or 2B Service, a service must meet as a minimum at least one condition relating to the number of users and at least one condition relating to functionality. For Category 2A Services, a service must meet as a minimum at least one condition relating to the number of users. This ensures that the factors which are set out on the face of the Bill as being most important in determining whether it is proportionate to place additional duties on the

provider of a user-to-user service or a search service will be reflected in each designation decision.

446 Under sub-paragraph (5) of paragraph 1, the Secretary of State, in making regulations under sub-paragraph (1) for Category 1 services, must consider the likely impact the factors set out in sub-paragraph (1) will have on how easily, quickly and widely user-generated content is disseminated by means of the service.

447 Under sub-paragraphs (6) and (7) of paragraph 1, the Secretary of State, in making regulations under sub-paragraphs (2) and (3), for Categories 2A and 2B, must consider the likely impact the factors set out in the previous sub-paragraphs will have on the level of risk of certain types of harm.

448 Paragraph 2 establishes the procedure for making 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. This 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. Extra time could be required if, for example, the Secretary of State determined that it were necessary to consider the effectiveness of the transparency reporting framework for Category 1 services before extending its scope.

449 OFCOM must then provide advice to the Secretary of State, based on their research, as to what they consider would be the appropriate threshold conditions (paragraph 2(5) of Schedule 11). In respect of Category 1, 2A and 2B threshold conditions, OFCOM may advise that the regulations should include other characteristics or factors in addition to number of users (and, for user-to-user services, functionalities), and what those other characteristics or factors should be.

450 If the regulations include provisions which differ 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 11).

451 After the regulations are made, OFCOM will be required to assess services which they consider 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 85(1)). Services become subject to Category 1, 2A or 2B duties by virtue of being added to the relevant part of the register.

452 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 regulations may only be amended or replaced by further regulations, once OFCOM have carried out further research.

453 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 consider appropriate.

454 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 appropriate, what those changes should be). Paragraph 3(7) notes that OFCOM must publish this advice as soon as reasonably practicable after providing it.

455 To ensure oversight of the process, paragraphs 3(8) and (9) impose duties on the Secretary of State to publish a statement explaining their decision if they take action which departs from OFCOM's advice.

Clause 86: Register of categories of certain Part 3 services

456 This clause imposes a duty on OFCOM to establish and publish a register of each regulated service that meets the various threshold conditions set out in Schedule 11 and will therefore be designated as a Category 1, 2A or 2B Service.

457 Subsections (5) and (6) set out how services should be treated if they meet the threshold conditions for different categories of service. This can happen either where a user-to-user service (with no search engine) meets both the Category 1 and Category 2B threshold conditions or in the case of a combined service. Where a user-to-user service meets both the Category 1 and Category 2B conditions, it is considered a Category 1 service, and added only to the Category 1 part of the register. As a combined service is a user-to-user service with a search engine part, it is possible that the user-to-user part of the service will meet the threshold conditions for Category 1 or Category 2B and, at the same time, the search engine will meet the threshold conditions for Category 2A. Where this happens, the service is considered both a Category 1 and Category 2A service or both a Category 2B and Category 2A service, and added to both relevant parts of the register. Where a service meets the threshold conditions for all three categories, it is considered both a Category 1 and a Category 2A service and added to these parts of the register.

458 Subsection (9) outlines that OFCOM must take steps to obtain or generate information in order to assess whether Part 3 services meet the threshold conditions.

Clause 87: Duty to maintain register

459 This clause sets out OFCOM's duties with regard 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 86.

460 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 they consider are likely to meet the amended thresholds set in the relevant regulations. They 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.

461 Subsection (4) requires OFCOM, at any other time, to assess those services which are not on the register, but which they consider 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.

462 Subsections (6) to (8) 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 they are satisfied, based on the evidence submitted by the provider in question, that there has been a change to the service or to regulations under paragraph 1 of Schedule 10 which appears likely to be relevant. Only if OFCOM are satisfied that this is the case are they obliged to assess the service and notify the provider of their decision. This ensures that OFCOM do not have to do a full assessment every time a request is made, which could create disproportionate burdens. If OFCOM assess the service and consider that they no longer meet the relevant threshold, OFCOM must remove them from the relevant part of the register.

463 Subsection (9) requires OFCOM to take reasonable steps to obtain or generate information or evidence to inform their assessments of services under this clause, in the same way as they are required to do for the original assessments undertaken when the register is first established.

464 Subsection (11) 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.

Clause 88: List of emerging Category 1 services

465 This clause confers a duty on OFCOM to create and publish a list of companies that are approaching the Category 1 thresholds. This will ensure that OFCOM proactively identifies rapidly scaling services and are ready to assess and add these companies to the Category 1 register without delay.

466 Subsection (1) states that OFCOM must comply with this duty as soon as is reasonably practicable after the regulations specifying Category 1 threshold conditions have come into force.

467 Subsection (2) sets out the conditions a service must meet to be added to the list.

468 OFCOM will be required to assess services against these conditions and prepare a list of emerging Category 1 services. Subsections 3–6 outline how OFCOM will publish and manage this list.

469 Subsection (7) sets out how OFCOM can obtain or generate the necessary information or evidence for the purposes of assessing services for this list.

Chapter 3: Risk assessments of regulated user-to-user services and regulated search services

Clause 89: OFCOM's register of risks, and risk profiles, of Part 3 services

470 Subsection (1) of this clause places a duty on OFCOM to identify and assess the risks of harm to individuals in the United Kingdom presented by in-scope services. These risk assessments must cover the risks of harm to individuals in the United Kingdom presented by illegal

content and content that is harmful to children. Risk assessments for user-to-user services must also cover the risks of harm presented by the use of such services for the commission or facilitation of priority offences. OFCOM must publish a register of risks of Part 3 services which reflects the findings of the risk assessments carried out.

471 Subsection (5) sets out that OFCOM must develop risk profiles for different groupings of regulated services to assist them in complying with their risk assessment and safety duties. OFCOM should categorise these services as they consider appropriate. This must take into account the services' characteristics, which include user base, business model, governance and other systems and processes (see subsection (11)), the risk levels, and any other relevant matters identified in its risk assessment.

Clause 90: OFCOM's guidance about risk assessments

472 This clause sets out OFCOM's duties to provide guidance for providers of regulated services to assist them with complying with their risk assessment duties.

473 The clause sets out the types of guidance that must be prepared, when the guidance must be prepared, and when it must be updated. The clause requires OFCOM to consult the Information Commissioner before producing any guidance.

Chapter 4: Information

Information power and information notices

Clause 91: Power to require information

474 This clause gives OFCOM the power to require the provision of information they require in order to discharge their online safety functions. For instance, OFCOM could use this power to require a service provider to share its risk assessment in order to understand how a service provider was identifying risks.

Clause 92: Information notices

475 This clause provides further information on OFCOM's information gathering powers. The clause sets out the information that can, and the information that must, be included in a notice requiring the provision of information and imposes a duty on the recipient of such a notice to comply with it.

476 The clause also clarifies that OFCOM may require the provision of information in any form; that OFCOM may cancel an information notice; and that a person to whom a document is produced, for example an OFCOM employee, can take copies of a document and require an explanation of it.

Clause 93: Requirement to name a senior manager

477 Criminal proceedings may be pursued against a named senior manager of a regulated service that fails to comply with an information notice (see clause 99). This clause provides OFCOM with the power to require, in an information notice, that an entity names a relevant senior manager who will then be responsible for ensuring the entity complies with the notice.

478 Subsection (4) defines a senior manager as an individual who plays a significant role in making decisions or the managing and organising of the entity's relevant activities, as defined in subsection (5).

Skilled persons' reports

Clause 94: Reports by skilled persons

479 Subsection (1) sets out the circumstances under which OFCOM can require a report from a skilled person. The first scenario is for the purpose of identifying and assessing a failure or a possible failure, by a provider of a regulated service to comply with a relevant requirement (as listed in subsection (12)). The second scenario, which applies only where OFCOM considers that the provider may be at risk of failing to comply with a relevant requirement, is for the purpose of developing OFCOM's understanding of this risk and ways to mitigate it. The third scenario is in relation to assisting OFCOM when the regulator is deciding whether to give a notice requiring a provider to use their best endeavours to develop or source technology dealing with CSEA content, or in deciding the requirements to be imposed by such a notice.

480 Subsections (3) and (4) set out that OFCOM may appoint a skilled person (an external third party with relevant expertise) to carry out a report and notify the provider, or, alternatively, OFCOM can give a notice to a 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.

481 Subsection (6) sets out that the service provider, their employees, their contractors and other providers have a duty to assist the skilled person in any way reasonably required to prepare the report. Subsection (7) states that the provider is liable to pay the skilled person directly for the production of the report, which can be recovered through the courts (subsection 9).

Investigations and interviews

Clause 95: Investigations

482 This clause relates to investigations by OFCOM into whether a provider of a regulated service has failed, or is failing, to comply with a requirement mentioned in subsection (2). Subsection (1) lays down that the provider must cooperate fully with the investigation.

483 Subsection (2) sets out that the requirements cover the list of duties and requirements in clause 119 (enforceable requirements) and any requirements imposed by a notice under clause 110(1) (notices to deal with terrorism content or CSEA content (or both)).

Clause 96: Power to require interviews

484 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 are carrying out an investigation into the failure, or possible failure, of a provider of a regulated service to comply with a relevant requirement.

485 Subsections (2) and (3) specify what information OFCOM must provide when giving an individual a notice to attend an interview and subsection (4) lists the individuals who can be required to attend an interview.

486 Subsection (5) states that OFCOM must give a copy of the notice to the provider of the service if they give a notice to an officer, a partner or an employee of the provider of the service.

487 Subsection (6) specifies that this clause does not require a person to disclose information that would be protected by legal professional privileges (or, in Scotland, to confidentiality of communications) in legal proceedings.

Powers of entry, inspection and audit

Clause 97: Powers of entry, inspection and audit

488 This clause refers to Schedule 12 to the Bill, which makes provision about powers of entry, inspection and audit.

Schedule 12: OFCOM's powers of entry, inspection and audit

Authorised persons

489 Schedule 12 sets out OFCOM's powers of entry, inspection and audit. Paragraph (1) states that OFCOM may authorise persons to exercise their powers of entry and inspection, carry out audits or apply for and execute a warrant.

Power of entry and inspection without a warrant

490 Paragraph 2, sub-paragraphs (1), (2) and (3) set out conditions on OFCOM's powers of entry without a warrant.

491 Sub-paragraphs (4),(5), and (6) list what an authorised person may do.

Notice requiring information or documents at inspection

492 Paragraph 3 sets out information about the process associated with an inspection notice.

Audit

493 Paragraph 4 relates to the function of an audit notice. An audit notice may require a regulated provider to take actions mentioned in sub-paragraph (2) to assist OFCOM's audit.

Conditions for issue of a warrant

494 Paragraph 5 deals with the conditions for the issue of a warrant by a justice for the inspection of premises by OFCOM.

Evidence of authority

495 Paragraph 6 states the requirements an authorised person must meet before exercising a power of entry under a warrant.

Powers exercisable by warrant

496 Paragraph 7 lists what a warrant may allow an authorised person to do.

Powers of seizure: supplementary

497 Paragraph 8 deals with powers of seizure (i.e. when a person executing a warrant seizes a document, record or other thing).

Further provision about executing warrants

498 Paragraphs 9 to 15 set out further provisions relating to the execution of a warrant.

Return of warrants

499 Paragraph 16 sets out provisions relating to the return of warrants.

Restrictions on powers

500 Paragraph 17 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.

Offences

501 Paragraph 18 lays down that a person commits an offence if the person intentionally obstructs a person acting under this Schedule or the person fails, without reasonable excuse, to comply with any requirement imposed under this Schedule or knowingly provides false information.

502 Sub-paragraph (2) sets out the penalty of fine and/or maximum sentences that can be imposed by the relevant criminal court on conviction.

Interpretation

503 Paragraphs 19 to 23 define "domestic premises", "premises", person "acting under this Schedule", "enforceable requirement", and "warrant" for the purposes of this Schedule. Paragraphs 23 and 23 provide clarification around interpretation when paragraph (5)(1) is applied in Scotland or Northern Ireland.

Information offences and penalties

Clause 98: Offences in connection with information notices

504 This clause sets out the criminal offences that can be committed in relation to information notices issued by OFCOM. It is an offence for such persons to:

a. fail to comply with OFCOM's information request;

b. provide false information to OFCOM in response to their information request;

c. provide encrypted information to OFCOM that it is not possible to understand in response to OFCOM's information request; and

d. suppress, destroy or alter information requested by OFCOM.

505 Subsection (8) provides for a subsequent court order requiring compliance with an information notice, where a person has been convicted of an offence.

Clause 99: Senior managers' liability: information offences

506 This clause sets out the criminal offences that can be committed by named senior managers in relation to their entity's information obligations. Senior managers who are named in a response to an information notice can be held criminally liable for failing to prevent the relevant service provider from committing an information offence.

507 Senior managers can only be prosecuted under this clause where the regulated provider has already been found liable for failing to comply with OFCOM's information request.

Clause 100: Offences in connection with notices under Schedule 12

508 This clause establishes offences in connection with notices under Schedule 12. It is an offence, in connection with audit notices, for persons to fail to comply with a requirement of an audit notice without reasonable excuse. It is also an offence to knowingly provide false information in response to an audit notice.

509 It is an offence in connection with inspection or audit notices for a person to intentionally suppress, destroy or alter information required to be provided to OFCOM.

510 Upon conviction of an offence under this clause, the court may, on the prosecutor's application, make an order requiring the convicted person to comply with a requirement of a notice under paragraph 3 of Schedule 12 or an audit notice.

Clause 101: Other information offences

511 This clause establishes additional information-related offences. It is a criminal offence for persons to:

a. intentionally obstruct or delay a person copying a document;

b. fail to attend or participate in an interview with OFCOM; and

c. knowingly or recklessly provide false information when being interviewed by OFCOM.

512 Upon conviction under this clause, the court may require the convicted person to comply with making a copy of a document or a requirement under clause 96 within a specified period.

Clause 102: Penalties for information offences

513 This clause establishes penalties for various information offences contained in clauses 98, 99, 100 and 101.

Disclosure of information

Clause 103: Co-operation and disclosure of information: overseas regulators

514 This clause grants OFCOM an express power for collaboration and information sharing with an overseas regulator, including by disclosing online safety information in order to facilitate an overseas regulator exercising their online safety functions, or to cooperate with any related

criminal investigations or proceedings. An overseas regulator is a person in a country outside the United Kingdom which exercises functions corresponding to OFCOM's online safety functions and the power only applies in relation to an overseas regulator specified in regulations made by the Secretary of State.

515 Under subsection (3), unless an overseas regulator has OFCOM's consent or is acting in accordance with an order of a court or tribunal, they cannot use the information disclosed under this power for another purpose, or disclose it further.

516 Subsection (4) provides that disclosure under this power does not breach any obligation of confidence owed by the person making the disclosure, or any other restriction on such disclosure, other than the exceptions specified in subsection (5).

517 Subsection (6) allows the Secretary of State to give a direction prohibiting the disclosure of information under this power for the purposes of overseas proceedings or overseas proceedings of any description specified in that direction.

Clause 104: Disclosure of information

518 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 their functions under the CA 2003, Broadcasting Act 1990 and Broadcasting Act 1996 cannot be disclosed without the consent of the business in question.

519 Subsection (2) has the effect that, subject to the specific exceptions in section 393 of the CA 2003, OFCOM cannot disclose information with respect to a business which they have obtained by exercising their powers under the Online Safety Act 2023 without the consent of the business in question.

520 Subsection (3) amends the list of exceptions in section 393 (2) of the CA 2003 so OFCOM can disclose information about a business, without its consent, for the purposes of any civil proceedings brought under the Online Safety Act 2023.

521 Subsection (4) has the effect that the section 393 CA 2003 restriction on disclosure does not apply to details of enforcement action under clause 127 or research or other information published under Schedule 8.

522 Similarly, subsection (5) 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 the Online Safety Act 2023.

Clause 105: Intelligence service information

523 This clause places a duty on OFCOM to consult the relevant intelligence service before OFCOM discloses or publishes any information they have received (directly or indirectly) from that intelligence service.

524 Subsection (1) sets out that OFCOM cannot disclose any information that they have received from an intelligence service, or information about an intelligence service, unless OFCOM have received consent from the intelligence service to disclose the information.

525 Subsection (2) states that if OFCOM discloses information as set out in subsection (1) to a person, then that person must not further disclose the information unless they have received consent from the intelligence service to do so.

526 Subsection (3) states that if OFCOM were to publish the documents set out in (a) and (b) which contain information set out in subsection (1), then OFCOM must remove or obscure the information that cannot be disclosed due to subsection (1) before the documents are published.

Clause 106: Provision of information to the Secretary of State

527 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.

528 Subsection (2) of this clause amends section 24B(2) of the CA 2003 so that, where information relating to a particular business has been obtained using a power under the Online Safety Act 2023, 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 for OFCOM to share information that 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).

529 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, for OFCOM to share information which is reasonably required by the Secretary of State and:

a. Was obtained by OFCOM using the power under clause 91 in order to determine a proposed threshold figure, which if met or exceeded by providers renders them liable to pay fees to OFCOM (the purpose under subsection (5)(c) of that clause); or

b. Was obtained by OFCOM using the power under clause 156(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 107: Amendment of Enterprise Act 2002

530 This clause amends Schedule 15 of the Enterprise Act 2002 to enable the Competition and Markets Authority to share information with OFCOM to facilitate the exercise of OFCOM's functions under the Online Safety Act 2023.

531 This clause adds the Online Safety Act 2023.3 to Schedule 15 of the Enterprise Act 2002 so that it is a 'specified enactment' for the purposes of Section 241(3)(b) of the Enterprise Act 2002.

This allows disclosure of certain kinds of information to OFCOM for the purposes of OFCOM's online safety functions.

Clause 108: Information for users of regulated services

532 The clause makes amendments to Section 26 of the Communications Act 2003 (CA 2003) which provides for publication of information and advice for various persons, such as consumers.

Clause 109: Admissibility of statements

533 Subsection (1) sets out the circumstances in which a statement given to OFCOM, in connection with OFCOM's power to require information under clause 91, OFCOM's power to require interviews under clause 96 or required under OFCOM's powers of entry and inspection under Schedule 12, may be used in evidence against the person who gave the statement.

Chapter 5: Regulated user-to-user services and regulated search services: notices to deal with terrorism content and CSEA content

Clause 110: Notices to deal with terrorism content or CSEA content (or both)

534 Chapter 5 provides the statutory basis for OFCOM's power to require a service provider to use accredited technology to tackle terrorism content and child sexual exploitation and abuse (CSEA) content and/or develop and source technology to tackle CSEA content.

535 Subsection (1) sets out that OFCOM may issue a notice to a service provider of a regulated user-to-user service or a regulated search service, when doing so is necessary and proportionate.

536 Subsections (2)(a) states that OFCOM may require a service provider of a regulated user-to-user service to use accredited technology to identify terrorism content communicated publicly (as defined in clause 207) and/or CSEA content on any part of the service. The service must take down that content without delay. The service may also be required to prevent this content from being made accessible to users at the outset, so that they do not encounter it, for example by preventing the content from being uploaded onto the platform.

537 Subsection (2)(b) states that OFCOM may require a service provider of a regulated user-to-user service to use its best endeavours to source or develop technology to identify and remove CSEA content on any part of the service or to prevent users from encountering this content. This technology must meet minimum standards of accuracy.

538 Subsection (3) states that OFCOM may issue a notice under this clause to search services, and subsection (4) makes clear that any notice given under subsections (2) or (3) can be issued to a provider that has both user-to-user functions and search functions.

539 Subsection (5) states that in removing terrorism or CESA content under subsections (2) and/or (3), providers may solely deploy accredited technology, or a combination of accredited technology and human moderators.

540 Subsection (6) refers to clause 111 and clause 112, which provides criteria that OFCOM must consider before issuing a notice to a service provider as set out in subsection (1) and states that OFCOM must issue a warning notice before issuing a Notice under this section.

Clause 111: Warning notices

541 This clause sets out the process that OFCOM must follow in issuing a warning notice.

542 Subsection (1) states that OFCOM may only issue a notice under clause 110 to a service provider once they have given a warning notice.

543 Subsection (2) provides the details that OFCOM must include when issuing a warning notice to use accredited technology and subsection (3) provides the details that OFCOM must include when issuing a warning notice to develop or source technology.

544 Subsection (4) sets out the process that OFCOM must follow when issuing a warning notice for a combined user-to-user and search service.

545 Subsection (5) states that a notice can only be issued by OFCOM once the period in which a company can make representations, as set out in a warning notice, has finished.

Clause 112: Matters relevant to a decision to give a notice under section 110(1)

546 This clause sets out the circumstances under which OFCOM may issue a notice to a service provider, and the conditions that must be met before the power can be used.

547 Subsection (1) states that OFCOM may only issue a notice, as set out in 110(1), when it is necessary and proportionate, and this section provides information to aid this decision making.

548 Subsections (2) and (3a) sets out matters that OFCOM must take into account when deciding whether issuing a notice to use accredited technology or a notice to develop or source technology is necessary and proportionate.

Clause 113: Notices under section 110(1): supplementary

549 Subsection (2) provides that where a service provider is already using technology on a voluntary basis, but this is not sufficiently effective, OFCOM can still intervene and require a service provider to use a more effective technology, or the same technology in a more effective way.

550 Subsections (3) and (4) specify that OFCOM can include in the notice a requirement for service providers to operate an effective procedure for users to challenge the removal of their content from the service.

551 Subsection (4A) states that if OFCOM decides that it is necessary and proportionate to issue a notice following representations from the company, the company must make proportionate alterations to the regulated service to ensure that the specified technology is effective when implemented.

552 Subsections (5) and (6) set out the information that must be contained within a notice to use accredited technology and the period it may last for. OFCOM may specify the way in which

the technology must be used on the service to effectively meet the aims of the notice and to meet the minimum standards of accuracy. This could include directions on how the technology should be implemented, including for example technical set up, human moderation requirements, or the image database to be used.

553 Subsection (7) states that a notice may only require a regulated provider to use accredited technology in relation to regulated services in the United Kingdom or regulated services that affect United Kingdom users. Any type of technology that is assessed by OFCOM, or a third party appointed by OFCOM, as meeting minimum standards of accuracy can be required under this power.

554 Subsections (9) and (10) explain that OFCOM will only be able to require the use of technologies, including those which have been developed or sourced in response to a notice, that have been assessed by either OFCOM, or a third party appointed by OFCOM, as meeting the minimum standards of accuracy for detecting terrorism and/or CSEA content as set out by the Secretary of State.

Clause 114: Review and further notice under section 110(1)

555 Subsection (2) and (3) set out that under clause 113(11), OFCOM also has the power to revoke the notice if there are reasonable grounds to believe that the provider is not complying with it. If a notice is revoked and the matters in clause 112 are considered, OFCOM can issue a further notice.

556 Subsection (4) requires OFCOM to review whether a service provider has complied with a notice to use accredited technology before the end of the notice, and to review a notice to develop or source technology by the last date that any steps are required have been taken.

557 Subsection (5) specifies what OFCOM must consider in their review of a service provider's compliance with a notice to use accredited technology. Subsection (6) specifies that following the review, and after consultation with the provider, OFCOM may give the provider a further notice if OFCOM consider that it is necessary and proportionate to do so, taking into account the matters set out in section 112. Under subsection (7), the conditions set out in subsections (3)-(6) apply again.

Clause 115: OFCOM's guidance about functions under this Chapter

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

559 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 their guidance when exercising these powers. Before preparing the guidance, OFCOM must consult the Information Commissioner.

Clause 116: OFCOM's annual report

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

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

562 Subsection (3) cross-refers to clause 147 which sets out provisions for OFCOM excluding confidential information from its published reports.

Clause 117: Interpretation of the Chapter

563 This clause sets out that the definitions of "terrorism content" and "CSEA content" used in Chapter 5 are the same as those used in Part 3.

Chapter 6: Enforcement Powers

Provisional notices and confirmation decisions

Clause 118: Provisional notice of contravention

564 This clause addresses the process of starting enforcement. OFCOM must first issue a "provisional notice of contravention" to an entity before they reach their final decision. This is required before OFCOM can reach a final decision that a regulated service has breached an enforceable requirement, and before OFCOM makes the final decision regarding any specific steps the service will be required to take and/or any financial penalty that will be imposed as a result.

565 The provisional notice of contravention must be sent to the relevant entity or person. This notice sets out OFCOM's provisional decision that an entity has breached its duties, sets out how it has failed, or is failing, and the evidence OFCOM have of this. The notification must detail any proposed requirements that the person must take to comply with the duty or requirement, or remedy the contravention and/or the financial penalties OFCOM intend to impose.

566 Subsection (8) establishes a process for recipients of provisional notices to make representations to OFCOM, and provide evidence in response to the provisional findings set out in the notice. OFCOM's notice has to explain this process, and give a deadline for providing representations. This process means that OFCOM can only reach a final decision after allowing the recipient the chance to make representations.

Clause 119: Requirements enforceable by OFCOM against providers of regulated services

567 This clause lists the "enforceable requirements". Failure to comply with these enforceable requirements can trigger enforcement action.

568 The enforceable requirements include, for example, duties to carry out and report on risk assessments, safety duties (including specific duties relating to children) and duties related to users' rights (freedom of expression and privacy).

Clause 120: Confirmation decisions

569 If, having followed the required process (see clause 118), OFCOM's final decision is that a regulated service has breached an enforceable requirement, OFCOM will issue a confirmation decision. This will set out OFCOM's final decision and will explain whether OFCOM requires the recipient of the notice to take any specific steps and/or pay a financial penalty.

Clause 121: Confirmation decisions: requirements to take steps

570 A confirmation decision may require a person to take specific steps to either come into compliance with their duties or remedy the breach that they have committed.

571 OFCOM must allow a reasonable period for the recipient to complete the required steps. However, subsection (5) provides that OFCOM can require immediate action when the recipient has breached its information duties (because it will already be on notice as to what is required).

572 Clause 124 allows OFCOM to require services to use a particular kind of "proactive technology" in their confirmation decisions, with certain constraints and safeguards. Proactive technology is defined in clause 202.

573 Subsection (3) says that these requirements can only relate to the operation of a regulated service within the United Kingdom, or in so far as it affects United Kingdom users of the service.

574 Subsection (4) sets out certain details that must be included in a confirmation decision which requires specific steps to be taken. This includes the steps that are required, OFCOM's reasoning and the recipient's appeal rights.

Clause 122: Confirmation decisions: risk assessments

575 This clause applies where OFCOM have found that a regulated provider has failed to carry out an illegal content or children's risk assessment properly or at all; and have identified a risk of serious harm which the regulated provider is not effectively mitigating or managing.

576 In such cases OFCOM can require the regulated provider to comply with the parts of its illegal content safety duties or children's safety duties that require the provider to mitigate and manage that risk of harm as if it had been identified in the relevant risk assessment. The intention is that the provider will be required to mitigate the risk that OFCOM have identified despite the provider itself not having identified the risk in its risk assessment. OFCOM will specify the date by which the regulated provider must take or use measures to comply with the duty in question.

577 The requirement to take these measures will apply until the regulated provider has fully complied with the relevant risk assessment duties.

Clause 123: Confirmation decisions: children's access assessments

578 This clause applies where OFCOM have found that a regulated provider has failed to properly carry out a children's access assessment.

579 In such cases, OFCOM can require a regulated provider to carry out or re-do the children's access assessment and would set a deadline for the completion of the assessment in the confirmation decision. The maximum period of time OFCOM can allow the service to complete the assessment is three months from the date of the confirmation decision (although this can subsequently be extended at OFCOM's discretion).

580 This clause also gives OFCOM the power to determine that a service is likely to be accessed by children where there is evidence that it is possible for children to access all or part of the service and the child user condition in clause 30(3) is met. (The child user condition is met if either: (a) a significant number of children are users of the service, or part of the service; or (b) the service, or part of it, is likely to attract a significant number of child users). If OFCOM determine that a service is likely to be accessed by children, the children's risk assessment duties in clause 24 and the children's safety duties in clause 25 will apply to the service. OFCOM will specify the date from which the duties would apply in their confirmation decision. OFCOM can also set out the circumstances in which their determination will cease to apply in their confirmation decision.

Clause 124: Confirmation decisions: proactive technology

581 This clause sets out when OFCOM may, in a confirmation decision, require a service to use a kind of "proactive technology" specified in the confirmation decision. The clause also sets out the matters OFCOM must consider before deciding to impose such a requirement.

582 OFCOM may only require the use of proactive technology on content which is communicated publicly. Therefore, subsection (8) provides that a confirmation decision which requires the use of such technology must identify the content, or parts of the service that include content, which OFCOM consider meets that description of communicated publicly.

583 Subsection (7) provides that OFCOM may set the requirement for the regulated service to review their use of any technology imposed in response to a confirmation decision.

584 "Proactive technology" is defined in clause 202.

Clause 125: Confirmation decisions: penalties

585 This clause allows OFCOM to impose financial penalties in their confirmation decision. These can be a single amount or a daily rate penalty if the failure is ongoing. Before imposing any financial penalty in their confirmation decision, OFCOM must set out the proposed amount(s) to the recipient in their provisional notice of contravention and allow the recipient the chance to make representations.

586 Certain details must be included in a confirmation decision which imposes a penalty. This includes OFCOM's reasons for imposing a penalty, the breaches that have attracted the penalty, a deadline for payment and the consequences of non-payment.

Penalty notices etc

Clause 126: Penalty for failure to comply with confirmation decision

587 This clause allows OFCOM to impose a financial penalty on a person who fails to complete steps that have been required by OFCOM in their confirmation decision. OFCOM can only impose a penalty under this clause if they have not imposed a daily rate penalty in respect of the same failure in its confirmation decision (to prevent the person being penalised twice for the same delay).

Clause 127: Penalty for failure to comply with notice under section 110(1)

588 This clause allows OFCOM to impose a financial penalty on a person who fails to comply with a notice issued under clause 110(1), which is a notice that requires technology to be implemented to identify and deal with terrorism content and/or CSEA content on a service.

Clause 128: Non-payment of fee

589 Clause 75 explains where OFCOM may require a provider of a regulated service to pay a fee. Schedule 10 also provides for fees to be charged to providers to enable OFCOM to recover costs they have incurred undertaking work which directly or indirectly prepares OFCOM for their future role as the online safety regulator. If a provider of a regulated service does not pay its fee, either under clause 75 or Schedule 10, to OFCOM in full, OFCOM may give that provider a notice specifying the outstanding sum and the date by which it must be paid.

590 Clause 128 allows OFCOM to give a penalty notice to a provider of a regulated service who does not pay the fee due to OFCOM in full. OFCOM may only impose such a penalty where they have first notified the provider that they propose to do so in a notice issued under this clause and then given the provider the opportunity to make representations. OFCOM must also be satisfied that the unpaid fee is outstanding.

Clause 129: Information to be included in notices under sections 127 and 128

591 This clause requires OFCOM to include certain information in penalty notices issued under clauses 127 and 128. For example, OFCOM must state the reasons why they are imposing a penalty, the amount of the penalty and any aggravating or mitigating factors. OFCOM must also state when the penalty must be paid.

Amount of penalties etc

Clause 130: Amount of penalties etc

592 This clause cross-refers to Schedule 13 which sets out details on the financial penalties that OFCOM may impose under this Bill, including the maximum amount that may be imposed. OFCOM are required to produce guidelines setting out how they determine penalty amounts.

Schedule 13: Penalties imposed by OFCOM under Chapter 6 of Part 7

Amount of penalties: principles

593 Paragraph 2 of Schedule 13 sets out the things that OFCOM must take into account when determining the size of the penalty. This includes any representations made by the person or

evidence provided by the person and the effects of the failure. OFCOM must also consider any steps taken by the person to comply with the requirements set out in the provisional notice, confirmation decision or penalty notice, and any steps taken to remedy the failure. Any penalty that OFCOM imposes must be considered by OFCOM to be appropriate and proportionate to the failure (or failures).

Limitation to type and amount of penalties previously proposed

594 Paragraph 3 of Schedule 13 confirms that a penalty imposed by a confirmation decision or penalty notice may not exceed the amount of the penalty, or (if relevant) be payable over a longer period than was proposed in the earlier notice about the same breach(es).

595 However, the limiting impact of earlier notices on subsequent penalties, as set out in paragraph 3 of Schedule 13, does not apply in relation to a penalty for which two or more entities are jointly and severally liable for the breach(es) (see paragraph 3(2)), unless the provisional notice and confirmation decision is given jointly (see Schedule 15).

Maximum amount of penalties

596 Paragraph 4(1) of Schedule 13 says 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" for the person's most recent complete accounting period.

597 Paragraphs 4(4)-(6) also includes further detail on how "qualifying worldwide revenue" will be calculated. The term "qualifying worldwide revenue" will be defined in a statement produced and published by OFCOM under section 76.

Maximum amount of penalties: group of entities

598 Schedule 15 sets out the circumstances when OFCOM may hold two or more entities jointly and severally liable for a breach. Paragraph 5 of Schedule 13 sets out how penalties are to be calculated in such a scenario.

599 Paragraph 5(3) states that the maximum penalty that OFCOM can impose in such cases is the greater of £18 million and 10% of the "qualifying worldwide revenue" of the group of entities of which the provider of the regulated service is a member.

600 Paragraph 5(4) defines the "qualifying worldwide revenue" for a group of entities.

601 "Qualifying worldwide revenue" will be set out in a statement produced and published by OFCOM under section 76. The statement must include provision about the application of that term to a group of entities.

Recovery of penalties

602 Paragraph 6 of Schedule 13 sets out how payment of penalties can be recovered and enforced.

Business disruption measures

Clause 131: Service restriction orders

603 The Bill gives OFCOM the power to apply to the courts for "business disruption measures". Business disruption measures are court orders that require third parties to withdraw services or block access to non-compliant regulated services. They are designed to only be used for the most serious instances of user harm. There are two types of business disruption measures: "service restriction orders" and "access restriction orders". The details and grounds for both are covered in clauses 131 to 134.

604 Clause 131 sets out the circumstances in which OFCOM may apply to the court for a "service restriction order". Service restriction orders are orders that require providers of "ancillary services" (persons providing, for example, payment or advertising services) to take steps aimed at disrupting the business or revenue of a non-compliant provider's operations in the United Kingdom. For example, an order could require an advertising service to cease the provision of its service to a non-compliant provider's service.

Clause 132: Interim service restriction orders

605 This clause sets out the circumstances in which OFCOM may apply to the courts for an "interim service restriction order". OFCOM can pursue an interim service restriction order in circumstances where it is not appropriate to wait for a failure to comply with an enforceable requirement to be established before making the order. OFCOM are not required to demonstrate to the court that a failure has been established (something which can take a long time), but must demonstrate that it is likely that the provider is failing to comply with a requirement under the Bill, and that the nature and severity of that harm mean that it would not be appropriate to wait to establish the failure before applying for the order.

606 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 court makes a service restriction order under clause 131 that imposes requirements on the persons who are subject to the interim service restriction order (or dismisses the application for such an order).

Clause 133: Access restriction orders

607 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, by preventing, restricting or deterring individuals in the United Kingdom from accessing that service. Examples of access facilities are internet service providers and app stores which may be required to restrict access to a service provider's website or app via their service.

608 In order to apply for an access restriction order, OFCOM must consider that a service restriction order under clause 131 or 132 would not be sufficient to prevent significant harm to individuals in the United Kingdom.

Clause 134: Interim access restriction orders

609 This clause sets out the circumstances in which OFCOM may apply to the courts for an interim access restriction order. OFCOM can seek to pursue an interim access restriction order in those circumstances where it is not appropriate to wait for the failure to be established before making the order (for example, if there is serious user harm that requires quick action to impede access). OFCOM are not required to demonstrate to the court that a failure has been established (something which can take a long time), but must demonstrate that certain conditions exist which mean that it would not be appropriate to wait to establish the failure before applying for the order.

Clause 135: Interaction with other action by OFCOM

610 This clause explains how business disruption orders interact with OFCOM's other enforcement powers. Where OFCOM exercise their powers to apply to the courts for business disruption orders under clauses 131 to 134, they are not precluded from taking action under their other enforcement powers.

Publication of enforcement action

Clause 136: Publication by OFCOM of details of enforcement action

611 If, having followed the required process (see clause 118), OFCOM's final decision is that a regulated service has breached an enforceable requirement, OFCOM will issue a confirmation decision under clause 120. This will set out OFCOM's final decision and will explain whether OFCOM require the recipient of the notice to take any specific steps and/or pay a financial penalty.

612 Where OFCOM issue a confirmation decision, they are obliged to publish the identity of the person to whom the confirmation decision was sent, details of the failure to which the confirmation decision relates and details relating to OFCOM's response.

613 OFCOM are also obliged to publish these details when they give a person a penalty notice for: failing to comply with a confirmation decision (under clause 126); failing to comply with a notice to deal with terrorism content or CSEA content (or both) (under clause 127); and failing to pay a fee in full (under clause 128).

614 This is intended to provide transparency in relation to OFCOM's enforcement activities.

Clause 137: Publication by providers of details of enforcement action

615 This clause gives OFCOM a power to require regulated services to publish the details, or otherwise notify UK users, of OFCOM's enforcement action. When using this power OFCOM must set out in a publication notice what enforcement decision or notice it is referring to, the detail that is to be published or notified, the form and manner in which it must be published or notified, the date by which is must be published or notified, as well as information about the consequences of not complying with the publication requirement.

616 This measure is intended to promote transparency by increasing awareness amongst users about providers' breaches of duties in the Bill.

Guidance

Clause 138: OFCOM's guidance about enforcement action

617 This clause requires OFCOM to publish guidance about how they will use their enforcement powers. This is intended to help regulated providers and other stakeholders understand how OFCOM will exercise their suite of enforcement powers.

Chapter 7: Committees, research and reports

Clause 139: Advisory committee on disinformation and misinformation

618 This clause places an obligation on OFCOM to form an advisory committee on disinformation and misinformation. This is 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.

Clause 140: Functions of the Content Board

619 The Content Board is a committee of the main OFCOM Board, with delegated and advisory responsibilities. This clause amends Section 13 of the Communications Act 2003 (functions of the Content Board) to clarify that it allows, but does not require, OFCOM to confer functions on the Content Board in relation to OFCOM's content related functions under the Online Safety Act 2023.

Clause 141: Research about users' experiences of regulated services

620 This clause amends Section 14 of the Communications Act 2003 (consumer research) to require OFCOM to arrange research into United Kingdom users' opinions and experiences relating to regulated services.

621 Subsection (2) provides that OFCOM must make arrangements to understand a number of factors, including public opinion concerning providers of regulated services and the experiences and interests of those using regulated services. The intention is to provide OFCOM with the flexibility to choose the most appropriate methods for such research. This subsection also provides that OFCOM must include a statement of the research they have carried out in their annual report to the Secretary of State and the devolved administrations, under paragraph 12 of the Schedule to the Office of Communications Act 2002.

Clause 142: Consumer consultation

622 This clause extends the Consumer Panel's remit to include online safety by amending Section 16 of the Communications Act 2003 (consumer consultation).

623 It ensures that the Consumer Panel is able to give advice on matters relating to different types of online content (under this Act) and the impacts of online content on United Kingdom users of regulated services.

Clause 143: OFCOM's statement about freedom of expression and privacy

624 This clause requires OFCOM to publish annual reports on the steps they have taken when carrying out online safety functions to uphold users' rights under Articles 8 and 10 of the Convention, as required by Section 6 of the Human Rights Act 1998.

Clause 144: OFCOM's reports about news publisher content and journalistic content

625 This clause requires OFCOM to publish a report about how the Bill's regulatory framework impacts on how news publisher and journalistic content is treated and made available by Category 1 services.

626 Subsection (1) specifies that the report should assess the impact of the regulatory framework on the availability and treatment of news publisher and journalistic content on Category 1 services.

627 Subsection (2) specifies that the report must be published within two years of the duties to protect news publisher content and journalistic content coming into force.

628 Subsection (3) specifies that the report must in particular pay attention to how effective the duties on Category 1 services to protect such content are.

629 Subsection (4) provides further detail on who OFCOM must consult when producing the report.

630 Subsection (5) specifies that OFCOM are required to send a copy of the report to the Secretary of State, who must lay it before Parliament.

631 Subsections (6) and (7) specify that the Secretary of State may require OFCOM to produce and publish further reports following the publication of the first report.

Clause 145: OFCOM's transparency reports

632 This clause creates a duty on OFCOM to produce their own reports based on information from the transparency reports that providers are required to publish. The intention is for the report to highlight key insights from the providers' reports, giving users a better understanding of the steps service providers are taking. The report must be published annually.

Clause 146: OFCOM's report about researchers' access to information

633 This clause requires OFCOM to publish a report about the access independent researchers have, or could have, into matters relating to the online safety of regulated services. The clause sets out what OFCOM's report must cover and requirements around consultation, parliamentary procedure and publication. OFCOM may also publish guidance relating to the content of the report

Clause 147: OFCOM's reports

634 This clause gives OFCOM a discretionary power to publish reports about certain online safety matters. OFCOM will need to consider excluding confidential matters from their reports to the

extent it is practicable. An example of this would be information that could be considered commercially sensitive.

Part 8: Appeals and super-complaints

Chapter 1: Appeals

Clause 148: Appeals against OFCOM decisions relating to the register under section 86

635 This clause allows for appeals against OFCOM's decisions to include, or not to remove, services from OFCOM's register of Category 1, Category 2A, and Category 2B services. Service providers who are registered by OFCOM as Category 1, Category 2A, and Category 2B services become subject to additional duties under the Bill.

636 Appeals may be made by regulated providers to the Upper Tribunal. The Upper Tribunal must apply the same principles as a court would when hearing an application for judicial review. The clause also lays down that where a regulated provider has filed an appeal, any additional duties or requirements applying under the Act associated with that provider being designated as a Category 1, 2A, or 2B operator need not be complied with until the determination or withdrawal of the appeal.

637 The Upper Tribunal may either dismiss the provider's appeal or quash OFCOM's decision. Should the Tribunal quash the decision then the Tribunal must remit the decision back to OFCOM.

Clause 149: Appeals against OFCOM notices

638 This clause allows for appeals against decisions by OFCOM to issue a confirmation decision, a notice under clause 110(1) or a penalty notice. An appeal may be brought to the Upper Tribunal by any person with 'sufficient interest' in the decision, although anyone other than the recipient requires permission from the Upper Tribunal to appeal.

639 The Tribunal will apply the same principles as a court would when hearing an application for judicial review.

640 The Upper Tribunal may either dismiss the appeal or quash OFCOM's decision. Should the Tribunal quash the decision then the Tribunal must remit the decision back to OFCOM for reconsideration, with any directions that the Tribunal thinks are appropriate.

Chapter 2: Super-complaints

Clause 150: Power to make super-complaints

641 This clause establishes a super-complaints mechanism which enables any organisation or other entity that meets the relevant eligibility criteria to bring systemic issues to OFCOM in specific circumstances.

642 A super-complaint can be about any feature of a regulated service or conduct of the provider of such a service. It may relate to one or more regulated services or providers and may be

about any combination of features and conduct. Where this feature, conduct or combination of the two is causing, appears to be causing or is at material risk of causing users or members of the public significant harm, significantly adversely affecting their right to freedom of expression, or having a significant adverse impact on them, an eligible entity may make a super-complaint.

643 Where a super-complaint relates to the conduct of a single regulated service or single provider of one or more regulated services, OFCOM may only consider it if they believe that the complaint is of particular importance or it relates to impacts on a particularly large number of people.

Clause 151: Procedure for super-complaints

644 This clause requires the Secretary of State to make regulations which set out the procedural aspects of complaints made under clause 150. It provides examples of the matters that these regulations may include provision for; for example, pre-notifying OFCOM of an organisation's intention to make a super-complaint.

645 The Secretary of State must consult OFCOM and anyone else they consider to be appropriate before making these regulations.

Clause 152: OFCOM's guidance about super-complaints

646 This clause puts a requirement on OFCOM to produce and publish guidance on super-complaints and sets out what the guidance must include.

Part 9: Secretary of State's functions in relation to regulated services

Strategic Priorities

Clause 153: Statement of strategic priorities

647 This clause introduces a power for the Secretary of State to set out a statement of the Government's strategic priorities in relation to online safety matters. 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.

648 Before designating the statement, the Secretary of State must first consult and follow the parliamentary procedure set out in clause 154.

649 The statement may specify particular outcomes to be achieved with a view to delivering 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 service providers.

650 If a statement of strategic priorities is to be amended in whole or in part, this must be done by issuing a subsequent statement following the procedure in clause 154. There are limited circumstances in which amendments may be made within a five year period, for example

where there has been a significant change in government policy affecting online safety matters.

Clause 154: Consultation and parliamentary procedure

651 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 153.

652 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.

653 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. They must then lay the draft statement before Parliament (subsection (4)) where it is subject to the negative resolution procedure as set out in subsections (5) - (7). After that procedure the Secretary of State may designate the statement.

Directions to OFCOM

Clause 155: Directions about advisory committees

654 This clause enables the Secretary of State to give OFCOM a direction to establish an expert committee to advise OFCOM on a specific online safety matter. By way of example, a direction could be issued requiring OFCOM to establish a committee to provide advice on an emerging online safety issue. The committee could do this by facilitating multi-stakeholder dialogue and building a greater understanding of the respective issue.

655 Subsection (3) sets out that OFCOM must appoint a committee chair, and that the number of additional members is at OFCOM's discretion unless the direction specifies otherwise in either case.

656 Subsection (4) places a duty on an advisory committee established under this direction to publish a report within 18 months of it being established, unless the direction specifies otherwise. After the initial report, the committee is required to publish reports periodically at their own discretion.

Clause 156: Directions in special circumstances

657 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 a specific threat when exercising its media literacy functions and to require specified service providers, or providers of regulated services generally, to publicly report on what steps it is taking to respond to that threat. For example, the Secretary of State could issue a direction during a pandemic to require OFCOM to: give priority to ensuring that health misinformation and disinformation is

effectively tackled when exercising its media literacy function; and to require service providers to report on the action they are taking to address this issue.

658 Subsection (6) specifies that the Secretary of State must publish the reasons for giving a direction in circumstances where this is given in response to a threat to the health or safety of the public. There is no requirement to publish reasons for giving a direction where this is done in response to a threat to national security.

659 The Secretary of State can vary or revoke a direction at any time. If so, OFCOM can vary or revoke the public statement notice they have given pursuant to the Secretary of State's direction: see subsection (7) and (8).

Guidance

Clause 157: Secretary of State's guidance

660 This clause enables the Secretary of State to give guidance to OFCOM relating to OFCOM's exercise of their statutory powers and functions under the Online Safety Bill. The guidance will provide clarity to OFCOM and others about how the Secretary of State expects OFCOM to carry out their statutory functions.

661 Subsections (3) to (7) detail the requirements for producing guidance issued under this clause.

662 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 158: Annual report on the Secretary of State's functions

663 Section 390 of the Communications Act 2003 requires the Secretary of State to prepare and lay before Parliament annual reports about their performance of the Secretary of State's functions under specific legislation, including the Communications Act 2003, the Office of Communications Act 2002 and the Broadcasting Acts 1990 and 1996.

664 This clause amends the Communications Act 2003 by adding the functions under the Online Safety Act 2023 to the list of functions which the Secretary of State must include in their annual report to Parliament.

Review

Clause 159: Review

665 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 3 are commenced, in order to assess the effectiveness of the regulatory framework. The timing requirement 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.

666 The review must consider a number of areas in assessing the effectiveness of the regulatory framework. These areas include how effective the regulatory regime has been at ensuring that

regulated services are operating, using systems and processes that minimise the risk of harm to individuals in the United Kingdom, and in providing higher levels of protection for children than for adults.

667 The Secretary of State is also required to take into account OFCOM's reports published under clause 144.

668 The review must also consider the effectiveness of: OFCOM's information gathering, information sharing and enforcement powers; and the extent to which OFCOM have had regard to the desirability of encouraging innovation.

Part 10: Communications offences

Harmful, false and threatening communications offences

Clause 160: False communications offence: England and Wales

669 This clause creates a criminal offence for the sending of false communications. A person who, without reasonable excuse, sends a message conveying information the person knows to be false, and in sending the message intends to cause psychological or physical harm that is more than trivial to those likely to encounter the message, is guilty of an offence.

670 The prosecution must prove beyond reasonable doubt that the sender lacked a reasonable excuse, and this assessment must include consideration of whether the message was or was intended as a contribution to a matter of public interest.

671 A person who commits an offence under this section is liable on summary conviction to imprisonment for a term not exceeding the maximum term for summary offences or a fine (or both). Subsection (6) sets out the definition of 'maximum terms for summary offences.'

672 This offence replaces the offence in section 127(2)(a) and (b) of the Communications Act 2003 and the offence in section 1(a)(iii) of the Malicious Communications Act 1988.

Clause 161: Exemptions from offence under section 160

673 This clause sets out exemptions for the false communications offence, including recognised news publishers. It also ensures that holders of broadcast or multiplex licences are exempt from committing the offence provided they are acting as authorised by the licence. Providers of an on-demand programming service are also exempt in connection with anything done in the course of providing such a service. Additionally, this clause also provides that an offence cannot be committed in connection with the showing of a film made for cinema to members of the public.

Clause 162: Threatening communications offence: England and Wales

674 This clause creates a criminal offence for the sending of threatening communications. A person who sends a message conveying a threat of death, serious injury, rape, assault by penetration, or serious financial loss, intending that those who encounter the message will fear the threat will be carried out (or is reckless as to that fact), is guilty of an offence.

675 With respect to threats of serious financial loss, it is a defence for a person to show that, first, the threat was used to reinforce a reasonable demand and, second, that they reasonably believed the threat was a proper means of reinforcing the demand. This is similar to the defence contained in section 1(2) of the Malicious Communications Act 1988.

676 A person who commits an offence under this section is liable on summary conviction to imprisonment for a term not exceeding the general limit in a magistrates' court or a fine (or both); on conviction on indictment, to imprisonment for a term not exceeding five years or a fine (or both).

677 This offence replaces the offence in section 1(1)(a)(ii) of the Malicious Communications Act 1988.

Clause 163: Interpretations of sections 160 to 162

678 This clause sets out how different aspects of the offences in clauses 160 and 162 should be interpreted.

679 Subsection (2) and (3) sets out the interpretations of the phrase "sends a message." Subsection (5) sets out the interpretation of the phrase "encounter" in relation to a message.

680 Subsection (4) sets out that a provider of an internet service is not regarded as a person who sends a message by virtue of providing that internet service.

681 Subsection (6) sets out that for the purposes of the offences it does not matter if the content of the message is created by the person who sends it. Subsection (7) sets out that a message can consist of or include a hyperlink to other content.

682 Subsection (8) sets out that in clauses 160 and 162 , references to the 'message' are to be read as including content accessed which a sender directs a recipient to. In this subsection, "sending" includes "giving".

683 Subsection (9) clarifies that for the offences captured in clauses 160 to 162, the date on which a person commits an offence in relation to a message is the date on which the message is first sent.

684 Subsection (10) sets out that "Recognised news publisher" is defined by section 50. Subsection (11) sets out the definition of "Multiplex licence." Subsection (12) sets out the definition of an "on-demand programme service".

Clause 164: Offences of sending or showing flashing images electronically: England and Wales and Northern Ireland

685 This clause creates two specific offences of sending or showing flashing images electronically to people with epilepsy intending to cause them harm. "Harm" means a seizure, or alarm or distress (subsection (13)).

686 Subsection (1) creates an offence of sending a communication by electronic means which consists of or includes flashing images, where one of two conditions set out in either subsection (2) or subsection (3) are met, without a reasonable excuse.

687 The condition set out in subsection (2) - condition 1 - is that, at the time the communication is sent, it is reasonably foreseeable that an individual with epilepsy would be among the individuals who would view the communication, and the communication is sent with the intention that such an individual will suffer harm as a result of viewing the flashing images. Condition 1 is intended to capture speculative messages sent to multiple people, for example on social media.

688 The condition set out in subsection (3) - condition 2 - is that, when sending the communication, the person sending it believes that an individual whom the sender knows or suspects to be an individual with epilepsy will, or might, view it and intends that individual to suffer harm as a result of viewing the flashing images. Condition 2 is intended to capture the more targeted sending of flashing images to an individual who the sender knows, or suspects, has epilepsy.

689 Subsection (4) provides that references in subsections (2)(a) and (3)(a) to viewing the communication include references to viewing a subsequent communication forwarding or sharing the content of the communication. The offence in subsection (1) may therefore be committed by a person who forwards or shares the electronic communication, as well as by the person sending it.

690 Subsection (5) provides that the exemptions contained in clause 161 also apply to an offence under subsection (1). This means that an offence of sending flashing images electronically cannot be committed: by recognised news publishers; by those with licences under the Broadcasting Acts 1990 or 1996; by the holder of a multiplex licence; by the providers of on-demand programme services; or in connection with the showing to members of the public of a film that was made for cinema.

691 Subsection (8) creates an offence of showing another person flashing images by means of an electronic communications device. The offence is committed if a person shows an individual flashing images, for example on a mobile phone screen, when showing the images knows or suspects that the individual concerned is an individual with epilepsy, intends that that individual will suffer harm as a result of viewing them, and if the person has no reasonable excuse for showing the images.

692 Subsection (9) provides an exemption for healthcare professionals acting in that capacity.

693 Subsection (10) provides that a person who commits an offence under subsection (1) or (8) is liable: on summary conviction in England and Wales, to imprisonment for a term not exceeding the general limit in a magistrates' court or a fine (or both); on summary conviction in Northern Ireland, to imprisonment for a term not exceeding six months or a fine not exceeding the statutory maximum (or both); and on conviction on indictment, to imprisonment for a term not exceeding five years or a fine (or both).

694 Subsection (11) provides that it does not matter whether images may be viewed immediately or only after some action, such as pressing play, is performed.

695 Subsection (12) provides that references to sending a communication or showing flashing images include references to causing a communication to be sent or causing flashing images to be shown.

696 Subsection (13) provides further definitions for the purposes of the section.

697 Subsection (14) provides that the clause extends to England and Wales and Northern Ireland.

Clause 165: Extra-territorial application and jurisdiction

698 Subsection (1) of clause 165 sets out that the offences established by clauses 160(1) and 162(1) can be committed outside the United Kingdom, though, in that case, only by an individual who is habitually resident in England and Wales or by a body incorporated or constituted under the law of England and Wales (subsection (2)).

699 Subsections (3) and (4) set out that the offence established by clause 164(1) can be committed outside of the United Kingdom, but only if the act is done by an individual who is habitually resident in England and Wales or Northern Ireland, or a body incorporated under the law of England and Wales or Northern Ireland.

700 Subsection (5) provides for courts in England and Wales to have jurisdiction over an offence under clause 160 or 162 that is committed outside the United Kingdom.

701 Subsection (6) provides for courts in England and Wales and Northern Ireland to have jurisdiction over an offence committed under clause 164(1) that is committed outside the United Kingdom.

Clause 166: Liability of corporate officers

702 Clause 166 establishes that offences under clauses 160, 162, or 164 can be committed by a body corporate or an officer of the body corporate. An "officer" in relation to a body corporate means a director, manager, associate, secretary or other similar officers; or a person purporting to act in any such capacity.

Offence of sending etc photograph or film of genitals

Clause 167: Sending etc photograph or film of genitals

703 Clause 167 creates a new offence of sending etc a photograph or film of a person's genitals to another person, in England and Wales. It inserts a new section 66A into the Sexual Offences Act 2003 ("the 2003 Act"). New section 66A(1) provides that where a person (A) intentionally sends or gives a photograph or film of any person's genitals to another person (B), and either A intends that B will see the genitals and be caused alarm, distress or humiliation, or sends or gives the photograph or film for the purpose of obtaining sexual gratification and is reckless as to whether B will be caused alarm, distress or humiliation, A commits an offence.

704 Subsection (2) makes clear that "sending or giving" a photograph or film includes, in particular, sending it to another person by any means, electronically or otherwise, showing it to another person, and placing it for a particular person to find.

705 Subsections (3) to (5) set out what is meant by "photograph" and "film". In particular, subsection (5) makes clear that the terms include an image, whether made by computer graphics or in any other way, which appears to be a photograph or film; a copy of such an image, photograph, or film, and data stored by any means which is capable of conversion into such an image; photograph, or film.

706 Subsection (6) provides that the offence is triable either way, and is subject to a maximum penalty of twelve months' imprisonment, a fine, or both, following summary conviction, and two years' imprisonment following conviction on indictment. The reference to twelve months' imprisonment is to be read as six months in relation to an offence committed before paragraph 24(2) of Schedule 22 to the Sentencing Act 2020 comes into force (new subsection (7)).

Repeals and amendments in connection with offences

Clause 168: Repeals in connection with offences under sections 160 and 162

707 Clause 168 sets out that subsection (2)(a) and (b) of the Section 127 of the Communications Act 2003 will be repealed in so far as they extend to England and Wales. Clause 168 also repeals section (1)(1)(a)(ii), section (1)(1)(a)(iii) and section (1)(2) of the Malicious Communications Act 1988.

Clause 169: Consequential amendments

708 Clause 169 sets out in which part of Schedule 14 the consequential amendments in connection with the offences created in clauses 160, 162, 164 and 167 can be found.

Schedule 14: Amendments consequential on offences in Part 10 of this Act

Part 1

Amendments consequential on offences in sections 160, 162 and 164

Football Spectators Act 1989

709 Paragraph 1 of Schedule 14 amends Schedule 1 of the Football Spectators Act 1989 (football banning orders: relevant offences) to reflect references to the new false and threatening communications offences under the Online Safety Act 2023.

Sexual Offences Act 2003

710 Schedule 5 of the Sexual Offences Act 2003 lists offences in connection with which a sexual harm prevention order may be made. Paragraph 2 of Schedule 14 adds to this list an offence under clause 160 of the Online Safety Act 2023 (false communications); and an offence under clause 162 of that Act (threatening communications).

Regulatory Enforcement and Sanctions Act 2008

711 Paragraphs 1 and 3 update Schedule 3 of the Regulatory Enforcement and Sanctions Act 2008, to include references to clause 160 and 162 (false communications and threatening communications offences).

Elections Act 2022

712 Paragraph 4 refers to the offences in Part 5 of the Elections Act 2022 (disqualification from holding elective office). The new false and threatening communications offences under this Bill, and the new offences of sending or showing flashing images electronically, are subsequently added.

Part 2

Amendments consequential on offence in section 167

Children and Young Persons Act 1933

713 Paragraph 5 amends Schedule 1 of the Children and Young Persons Act 1933 (offences against children and young persons with respect to which special provisions of Act apply) to refer to section 66a in the entry relating to the Sexual Offences Act 2003.

Sexual Offences Act 2003

714 Paragraph 6 amends the Sexual Offences Act 2003. Subparagraph (2) amends section 136A(3A) (specified child sex offences), and inserts "66A" in paragraph (c).

715 Sub-paragraph (3) inserts a clause into Schedule 3 (sexual offences for purposes of Part 2), paragraph 33A, referring to an offence under section 66A of that Act (sending etc photograph or film of genitals) in specific circumstances.

Criminal Justice Act 2003

716 Paragraph 7 amends the Criminal Justice Act 2003 to refer to an offence under section 66A of the Sexual Offences Act 2003 (sending etc photograph or film of genitals) in Part 2 of Schedule 15 (specified sexual offences for purposes of section 325) and Schedule 34A (child sex offences for purposes of section 327A).

Anti-social Behaviour, Crime and Policing Act 2014

717 Paragraph 8 amends section 116 of the Anti-social Behaviour, Crime and Policing Act 2014 (information about guests at hotels believed to be used for child sexual exploitation) to add a reference to section 66A in the entry that relating to exposure and voyeurism offences in the Sexual Offences Act 2003.

Modern Slavery Act 2015

718 Paragraph 9 amends Schedule 4 of the Modern Slavery Act 2015 (offences to which defence in section 45 does not apply) to refer to section 66A under paragraph 33 (offences under Sexual Offences Act 2003).

Sentencing Act 2020

719 Paragraph 10 amends Part 2 of Schedule 18 to the Sentencing Act 2020 (specified sexual offences for purposes of section 306) to refer to section 66A under paragraph 38 (offences under Sexual Offences Act 2003).

Elections Act 2022

720 Paragraph 11 amends Schedule 9 of the Elections Act 2022 (offences for the purposes of Part 5) to refer to section 66A (sending etc of photograph or film of genitals).

Part 11: Supplementary and General

Providers' judgements about the status of content

Clause 170: Providers' judgements about the status of content

721 This clause clarifies how providers are to approach judgements (human or automated) about whether content is content of a particular kind (such as illegal content, content that is harmful to children, etc), when their risk assessments or systems and processes for compliance with the Act involve such judgments. In particular, it makes provisions about how questions of mental state and defences are to be approached when considering whether content is illegal content or a fraudulent advertisement.

722 Subsection (2) requires that such judgments must be made on the basis of all the relevant information that is reasonably available to a provider.

723 Subsection (3) specifies factors that are particularly relevant to the question of what information is "reasonably available" to a provider. It makes clear that the requirement in subsection (2) applies both to judgements made by human moderators and those made by automated systems and processes, but that the information reasonably available to an automated system or process, might be construed to be different to the information reasonably available to human moderators.

724 Subsections (5) and (6) apply specifically to judgements about whether content is illegal content or a fraudulent advertisement. Providers must treat content as illegal content or a fraudulent advertisement if, on the basis of all information reasonably available to the provider, there are reasonable grounds to infer all the elements - including mental elements such as intention - necessary for the commission of the offence are present, and there are not reasonable grounds to infer a defence may be relied upon.

725 Subsection (7) makes provision for judgements about whether content that is generated by bots is illegal content or a fraudulent advertisement, including in particular how providers should consider mental elements and defences relating to content generated by bots. Clause 49(4) of the Bill sets out that content generated by bots can be 'user-generated content' for the purposes of the Bill, and so can be in-scope of Part 3 services' duties.

Clause 171: OFCOM's guidance about illegal content judgements

726 This clause requires OFCOM to produce guidance for providers about how they should approach judgements about whether content is illegal content or a fraudulent advertisement.

727 Subsections (3) and (4) require that OFCOM must consult appropriate persons before creating the guidance, and must publish the guidance.

Liability of providers etc

Clause 172: Providers that are not legal persons

728 This clause provides for the situation in which a penalty notice or confirmation decision needs to be given to a provider of a regulated service that is not a legal person. This may occur, for example, where a partnership or an unincorporated association (an organisation set up through an agreement between a group of people who come together for a reason other than to make a profit, such as a voluntary group or a sports club) provides a regulated service.

Clause 173: Individuals providing regulated services: liability

729 This clause sets out how various provisions of the Bill may apply to a group of two or more individuals who together are providers of a regulated service. Where two or more individuals together are providers of a regulated service, they will be jointly and severally liable for any duty, requirement or liability to pay a fee. Two or more individuals jointly given a penalty notice or confirmation decision will also be jointly and severally liable to pay the penalty or meet the requirements.

730 The clause also provides for how penalty notices or confirmation decisions may be given to individuals who are together providers.

Clause 174: Liability of parent entities etc

731 This clause cross-refers to Schedule 15, which contains provisions about how joint liability operates under the Bill.

Schedule 15: Liability of parent entities etc

Joint provisional notices of contravention

732 Schedule 15 establishes that decisions or notices can be given jointly to both a regulated provider and its parent company (or controlling individual(s)), its subsidiary company or a fellow subsidiary.

733 All relevant entities must be given the opportunity to make representations when OFCOM are seeking to establish joint liability, including on the matters contained in the decision or notice and whether joint liability would be appropriate.

734 When OFCOM issue decisions or notices to multiple parties, they are all jointly liable to comply with any requirements or penalties imposed.

Clause 175: Former providers of regulated services

735 This clause makes clear that OFCOM's powers to issue enforcement notices, including notices relating to the duty to cooperate with an investigation, may be given to a former provider of a regulated service. OFCOM can issue an enforcement notice to a former service provider if, at the relevant time, the provider was operating a regulated service.

Offences

Clause 176: Information offences: supplementary

736 This clause sets out further detail on how the information offences in clause 98(1) and paragraph 18(1)(b) of Schedule 12 operate.

737 Proceedings against a person for an offence of failing to comply with requirements in an information notice or failing to comply with any requirement imposed by a person authorised by OFCOM to exercise powers of entry and inspection may be brought only if:

a. The person has been given a provisional notice of contravention;

b. They have received a confirmation decision in respect of that failure (requiring them to comply with the original requirement or remedy their failure to comply with it) and they have not complied with its requirements by the deadline it sets;

c. A penalty has not been imposed on them by OFCOM in respect of that failure; and

d. Neither a service restriction order nor an access restriction order has been made in relation to a regulated service provided by them in respect of that failure.

738 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, these conditions must also be met in relation to the failure to comply with an information notice.

Clause 177: Defences

739 This clause applies where a person relies on a defence under clause 98 or 99.

740 Where a defendant adduces evidence which raises an issue with respect to the defence, the burden is on the prosecution to prove beyond reasonable doubt that the defence is not satisfied.

Clause 178: Liability of corporate officers for offences

741 This clause means that in certain circumstances 'corporate officers' of regulated providers may be found liable for information offences committed by that entity. Corporate officers are generally directors, managers or similarly senior employees.

742 If an offence is found to be committed by an entity, and that offence is proved to have been committed with the consent, connivance or neglect of a corporate officer, both the officer and the relevant entity can be found guilty of the offence.

Clause 179: Application of offences to providers that are not legal persons

743 This clause sets how information offences apply to providers that are not legal persons under the law under which they are formed. Under English and Welsh law, a partnership and an unincorporated association would both be examples of such entities.

744 Subsection (2) specifies that proceedings for an offence under this Act alleged to have been committed by a relevant entity must be brought against the entity in its own name. It must not

be brought in the name of any of its officers, members or partners. 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. A fine imposed on a relevant entity on its conviction of an offence under this Act is to be paid out of the entity's funds.

745 Subsection (5) provides that, if the relevant entity commits an offence, and this offence was committed with the consent or connivance of, or can be attributed to the neglect of, an officer, then the officer also commits the offence. Proceedings may thus be brought against the officer (subject to clause 176(1))and they may be punished accordingly. The liability of an officer under this subsection is not prejudiced by subsection (2).

Extra-territorial application

Clause 180: Extra-territorial application

746 This clause specifies that references to internet services, user-to-user services and search services and OFCOM's information-gathering powers apply to services provided from outside the United Kingdom (as well as to services provided from within the United Kingdom).

Clause 181: Information offences: extra-territorial application and jurisdiction

747 This clause outlines that the information offences in the Bill apply to acts done in the United Kingdom and outside of the United Kingdom. All offences can be prosecuted in any part of the United Kingdom as if they occurred in that part of the United Kingdom.

Payment of sums into the Consolidated Fund

Clause 182: Payment of sums into the Consolidated Fund

748 Clause 182 amends section 400 of the Communications Act 2003 so that it applies to amounts paid to OFCOM in respect of penalties imposed under the Online Safety Act 2023, and in respect of fees charged under Schedule 10. This clause requires OFCOM to pay any penalty sums, and any fees under Schedule 10, they receive into the Consolidated Fund of the United Kingdom.

Publication by OFCOM

Clause 183: Publication by OFCOM

749 This clause requires OFCOM to publish anything they must publish under the Bill in a way which is appropriate to bring it to the attention of any audience likely to be affected by it.

Service of notices

Clause 184: Service of notices

750 This clause sets out the process for serving any notices or decisions under the Act, including notices to deal with CSEA or terrorism content, information notices, enforcement notices, penalty notices and public statement notices to providers of regulated services both within and outside of the United Kingdom.

Repeals and amendments

Clause 185: Amendments of Part 4B of the Communications Act

751 This clause introduces a new Schedule (Amendments of Part 4B of the Communications Act) to amend the Video-Sharing Platform (VSP) regime contained in Part 4B of the Communications Act to ensure the regime remains effective until it is repealed.

Schedule 16: Amendments of Part 4B of the Communications Act

752 This schedule makes amendments to Part 4B of the Communications Act, which regulates Video-Sharing Platform (VSP) services, to address changes required to the United Kingdom's VSP regime as a result of the United Kingdom's exit from the EU and to ensure the regime remains effective until it is repealed. Amendments include removing references to EU law, and allowing OFCOM to cooperate with EEA states.

Clause 186: Repeal of Part 4B of the Communications Act

753 This deletes clauses pertaining to the regulation of Video-Sharing Platform services from the Communications Act 2003, the Audiovisual Media Services Regulations 2020 and the Audiovisual Media Services (Amendment) (EU Exit) Regulations 2020.

Clause 187: Repeal of Part 4B of the Communications Act: transitional provision etc

754 This clause introduces Schedule 17 (Video-Sharing Platform services: transitional provision etc) which contains transitional, transitory and savings provisions relating to the repeal of the Part 4B of the Communications Act 2003, which contains the regulatory regime for the regulation of Video-Sharing Platform services. This clause also gives the Secretary of State a power to make regulations containing further transitional, transitory or savings provisions.

Schedule 17: Video sharing platform services: transitional provision etc

755 This Schedule contains transitional, transitory and saving provisions setting out how the Video-Sharing Platform (VSP) regime in Part 4B of the Communications Act 2003 will be repealed and how the Online Safety Act 2023 will apply during the "transitional period".

756 Part 2 of Schedule 17 sets out that the Online Safety Act 2023 will apply to VSPs (that meet the definition set out in Schedule 17, paragraph 1); however, for the duration of the transitional period, they will be exempted from certain Online Safety Act 2023 duties and requirements. During this transitional period, these VSPs will continue to be regulated under the VSP regime. Broadly, where an internet service is wholly a VSP (Schedule 17, paragraph 1(1)(a)), the exemption applies to the service as a whole. However, where only a "dissociable section" of an internet service is a VSP (Schedule 17, paragraph 1(1)(b)), the exemption will only apply to the VSP part. However, VSPs will still be subject to the new communications offences, OFCOM's information powers and associated enforcement powers, and fee notification requirements. VSPs will also become subject to the requirement to complete children's access and risk assessments once a date is specified by the Secretary of State via regulations.

757 Part 3 of Schedule 17 sets out the application of Part 6 of the Online Safety Act 2023 in respect of transitional charging years. The transitional arrangements require that VSPs provide

notification of eligibility to pay fees and provide financial information to OFCOM under clause 74.

758 Where a VSP is an "exempt provider", the provider does not have to pay fees under clause 75 or Schedule 10, during a transitional charging year. Where a VSP is not an "exempt provider" (i.e. it is an internet service with a "dissociable section" that is a VSP, and it has either another user-to-user part or search engine part that is not a VSP), if Schedule 17 paragraph 17(2) applies, their fee notification must include a breakdown indicating the amounts that are wholly referable to the VSP part. If a VSP is not an exempt provider, they are subject to the duty to pay fees under clause 75 or Schedule 10 in respect to a transitional charging year.

759 In calculating providers fees, the qualifying worldwide revenue (QWR) is to be taken as the "non-Part 4B QWR" i.e. the QWR less the amounts wholly referable to the VSP part. As per clause 75(3), in the event of a disagreement between the provider and OFCOM regarding the "non-Part 4B QWR" or fees payable, the amount is determined by OFCOM.

760 The transitional arrangements for VSPs will end on the date on which clause 186 of the Bill, which repeals Part 4B of the Communications Act 2003, comes into force (with the exception of Schedule 17, Part 3, which applies in respect to a transitional charging year). Clause 211(4) ensures that Part 4B may not be repealed until at least 6 months after the chosen date for the obligation to conduct risk and child access assessments (to give providers time to do their assessments before they become subject to the safety duties).

761 The savings provisions in Schedule 17, Part 4 will allow OFCOM to continue to pursue ongoing enforcement action, relating to breaches of Part 4B of the Communications Act 2003 that occurred while it was in force, after the repeal of that Part.

Clause 188: Repeals: Digital Economy Act 2017

762 This clause repeals 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 online service providers by repealing section 103 of that Act. As a consequence of the repeal of Part 3, the power to extend it to the Channel Islands or the Isle of Man is also repealed.

Clause 189: Offence under the Obscene Publications Act 1959: OFCOM defence

763 This clause amends Section 2 of the Obscene Publications Act 1959, to create a defence for employees of OFCOM and those assisting OFCOM in the exercise of OFCOM's online safety functions regulatory functions under the Online Safety Act 2023.

764 It inserts an additional subsection into the 1959 Act to create a defence for the offence of publishing an obscene article the effect of which is to tend to deprave and corrupt persons who are likely to read, see or hear the matter contained or embodied in it. This applies where the defendant is a member of OFCOM, employed or engaged by OFCOM or assisting OFCOM in the exercise of their online safety functions and the publication of the obscene article is made for the purpose of any of OFCOM's online safety functions, as defined in Clause 206.

765 We expect that the handling of this material may be necessary in the course of OFCOM's delivery of their online safety functions, as services will be required by duties in the legislation to proactively identify and remove this content. For example, OFCOM may be required to handle this material when assessing a services' systems and processes to assess how they handle illegal content.

Clause 190: Offences regarding indecent photographs of children: OFCOM defence

766 This clause amends Section 1B of the Protection of Children Act 1978 (defence to offence relating to indecent photographs of children) to create a defence for OFCOM when exercising their online safety functions.

767 It inserts an additional clause into the 1978 Act to create a defence for the offence of making an indecent photograph or pseudo-photograph of a child in circumstances where the defendant is a member of OFCOM, employed or engaged by OFCOM or assisting OFCOM in the exercise of their online safety functions and the photograph or pseudo-photograph is made for the purpose of any of OFCOM's online safety functions, as defined in clause 206. We expect that the handling of this material may be necessary in the course of OFCOM's delivery of their online safety functions, as services will be required by duties in the legislation to proactively identify and remove this content. An example of a scenario in which OFCOM may be required to handle this material would be if OFCOM is assessing a services' systems and processes to assess how they handle illegal content or needs to show that a service is not handling complaints about illegal content correctly.

768 The clause provides for amendment to the equivalent legislation in Scotland (Section 52 of the Civic Government (Scotland) Act 1982 (indecent photographs of children)) and in Northern Ireland (Article 3A of the Protection of Children (Northern Ireland) Order 1978 (defence to offence relating to indecent photographs of children)).

Powers to amend Act

Clause 191: Powers to amend section 35

769 This clause gives the Secretary of State the power to amend the list of fraudulent offences in clause 35 in relation to the duties about fraudulent advertising. This power is subject to some constraints.

770 Subsection (2) lists the criteria any further offence must meet before the Secretary of State may include it in the list of fraudulent offences in clause 35. Subsection (3) further limits the Secretary of State's power to include new fraud offences, listing types of offences which may not be added to clause 35. This is to avoid regulatory duplication.

Clause 192: Powers to amend or repeal provisions relating to exempt content or services

771 This clause allows the Secretary of State to make regulations to amend or repeal provisions relating to exempt content or services. Regulations made under this clause can be used to exempt certain content or services from the scope of the regulatory regime or to bring them into scope.

772 The provisions relating to exempt content or services cannot be amended so that comments on news publisher sites become regulated user-generated content.

Clause 193: Powers to amend Part 2 of Schedule 1

773 Schedule 1, paragraph 10 exempts user-to-user or search services that are provided by education or childcare providers as described in Schedule 1, Part 2, from regulatory duties where those services are provided for the purpose of education and childcare. Clause 192 provides a set of powers to amend the list of exempt education and childcare providers listed in Schedule 1 Part 2. This includes powers for the Secretary of State to amend the list in Part 2 Schedule 1 which relates to England (Clause 193(1)) and for the relevant Devolved Ministers to amend the list in their respective areas. This clause also sets out the criteria that must be met in order for an amendment to be made.

Clause 194: Powers to amend Schedules 5, 6 and 7

774 This clause gives the Secretary of State power to amend the three Schedules which list the criminal offences that are priority offences, as defined in clause 53(7).

775 The Secretary of State may amend the list of terrorism offences and the list of CSEA offences other than those CSEA offences which extend only to Scotland, which may be amended by the Scottish Ministers. The Secretary of State may also amend Schedule 7 (priority offences), but the Secretary of State may only add an offence to Schedule 7 if the Secretary of State considers it appropriate for the reasons set out in subsection (4) and the amendment would not add an offence of a type listed in subsection (6). The Secretary of State must consult with Scottish Ministers before making changes to offences in Schedule 7 that only extend to Scotland, and with the Department of Justice in Northern Ireland before making changes to offences that only extend to Northern Ireland.

Regulations

Clause 195: Power to make consequential provision

776 This clause gives the Secretary of State a power to make consequential provisions relating to this Bill or to regulations under this Bill. The power is exercised by regulations and includes the power to amend the Communications Act 2003.

777 This power cannot be exercised so as to include comments and reviews on content on services provided by recognised news publishers within the definition of "regulated user-generated content", and the power to amend Paragraph 4 of Schedule 1 (limited functionality services) cannot be exercised so as to remove such services which are provided by recognised news publishers from that exemption.

Clause 196: Regulations: general

778 This clause sets out how the powers to make regulations conferred on the Secretary of State can be used. Regulations made under this Act can make different provisions for different purposes, in particular relating to different types of services.

Clause 197: Parliamentary procedure for regulations

779 This clause sets out the Parliamentary procedure that must be followed when regulations made using powers conferred by the Bill are made.

Part 12: Interpretation and final provisions

Interpretation

Clause 198: "Provider" of internet service

780 This clause determines who is the 'provider' of an internet service, and therefore who is subject to the duties imposed on providers. For user-to-user services, subsections (2) and (3) set out that the provider is the entity (or individual(s)) that controls who can use the user-to-user elements of a service. The duties will therefore apply to the entity or person that directly controls users' access to the functionality that enables users to interact or share user-generated content, rather than on any other entity that may embed that service or control other aspects of it. This also makes clear to which entity within a broader corporate structure the duties apply.

781 Subsections (4) and (5) set out that a provider of a search service is the entity (or individual(s)) that has direct control over the operations of the search engine. As set out in subsection (13), 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. The duties will therefore apply to the person or entity that controls which search results appear to users and how they appear, rather than on any other entity that may embed or otherwise use a search engine.

782 Subsections (6) and (7) provide that the provider of a combined service is the entity which meets both definitions in the preceding four subsections. If the entity (or individual(s)) which controls who can use the user-to-user part of the service is different from the entity (or individual(s)) which controls the search engine, it will not be a combined service (see the definition of "combined service" in clause 3(7)).

783 Subsections (8) and (9) provide that the provider of an internet service which is neither a user-to-user service nor a search service is the entity (or individual(s)) which has control over which content is published or displayed on the service. This is relevant for determining which entities have duties under Part 5.

784 Subsection (12) 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 126(10)), is not a provider of that service. This therefore excludes companies which provide infrastructure to other services on a business-to-business basis.

785 Examples of "access facilities" include internet access services, web hosting services, domain name services, software as a service products, security software, content delivery network services, app stores, payment service providers and enterprise software.

Clause 199: "User", "United Kingdom user" and "interested person"

786 This clause defines the terms "user", "United Kingdom user", and "interested person", in relation to regulated services.

787 Subsection (1) makes clear that a "United Kingdom user" can be either 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.

788 Subsections (3) and (4) outline the circumstances where someone would not be counted as a user because they are using the service in the course of the service provider's business. For example, the intention is that an employee of a social media company would not count as a user if uploading content to the service in the course of their employment, for example a company blog. However, they would count as a user of the service if uploading content to that service in a personal capacity.

789 Subsection (7) defines an "interested person" in relation to search services and combined services. This is intended to recognise that these services' actions may affect people and entities who do not directly use search engines where search engines index their website or database.

Clause 200: "Internet service"

790 This clause sets out the meaning of the term "internet service", which includes services made available by the internet, or by a combination of the internet and an electronic communications service (as defined in Section 32(2) of the Communications Act 2003). 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. This captures services accessed by a mobile phone application as well as those accessed via an internet web browser.

Clause 201: "Search engine"

791 This clause sets out the meaning of "search engine". This is relevant to the definition of "search service" in clause 2(4), which is an internet service that is, or includes, a search engine.

792 Subsection (1)(a) 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 included. A vertical search engine is a search engine that is only focused on a specific topic or a genre of content, such as a search engine that only indexes academic articles. Subsection (1)(b) clarifies that the definition does not include services where a user can only search one website or database, thereby ensuring that websites which only have a search tool internal to the website are not considered search services.

793 Subsection (2) makes clear that for a service to be a combined service it is necessary for the entity which would be defined as the provider in relation to the user-to-user part of the

service to be the same as the entity which would be defined as the provider in relation to the search engine (although a single entity may be the provider of more than one service).

Clause 202: "Proactive technology"

794 Proactive technology may be used by regulated service providers to comply with their duties about illegal content, content which is harmful to children and fraudulent advertising. As explained in relation to those duties, the service provider must specify in their terms of service or publicly available statement if they use proactive technology. OFCOM may recommend the use of proactive technology in the codes of practice related to these duties (see Schedule 4, Paragraph 12), and may also impose confirmation decisions requiring the use of proactive technology (see clause 124). Both actions by OFCOM are subject to certain constraints included in Schedule 4 and clause 124, including considering the extent to which they might result in interference with users' right to freedom of expression within the law.

795 This clause provides a definition of proactive technology. Proactive technology consists of three types of technology for the purposes of this legislation, content moderation, user profiling and behaviour identification. The clause gives limited examples of the types of technologies that regulated services will use, and makes clear that this will in some cases include artificial intelligence and machine learning technologies.

796 Content moderation technology includes technology such as keyword matching or image classification, which will involve, for instance, automatically analysing user-generated content across a user-to-user service for the purposes of assessing if this is illegal content. The service provider can then decide what action is required in respect of that content to comply with its safety duties about illegal content (clause 9). Accredited technology required in relation to the detection of terrorism content or CSEA content (see clause 110) is also an example of content moderation technology. Technology which reviews content which has been flagged by a user report does not fall within this category.

797 User profiling technology refers to tools which build a profile of the user, assessing characteristics, so that the service provider can limit their access to harmful content if necessary. The provision notes that this will involve the analysis of content and user data, or relevant metadata of content and user data, which means this includes looking at a number of factors, such as what they post and view online, and could include data the service provider has from a partner site, for example. This doesn't include technology that checks data (such as ID) provided by the user to verify age.

798 Behaviour identification technology is a category of technology which assesses harmful behaviour online, including criminal activity. This also concerns the analysis of content and user data, or relevant metadata of content and user data. The provision clarifies that this does not mean investigations conducted by service providers into specific users, where technology is used in response to concerns identified by another person (or another automated tool). Subsection (9) defines user data, which is a category of data which these tools will analyse in addition to content and metadata. It specifies that this will include personal data, as well as data that the service provider will create about user activity, or obtain from partner services.

Clause 203: Content communicated "publicly" or "privately"

799 This clause provides information to assist OFCOM in their decision making on whether content is communicated publicly or privately for the purposes of exercising its powers under the Bill.

800 Subsection (1) sets out that OFCOM must consider the factors listed in this clause relating to the functionality and design of the service when making decisions on whether content is communicated publicly or privately under clauses 110 and 124 and under Schedule 4.

801 Subsection (2) sets out the factors that OFCOM must consider in their decision making.

802 Subsection (3) sets out the factors that OFCOM should not consider as being restrictions on users accessing a service.

Clause 204: "Functionality"

803 This clause sets out the meaning of the term 'functionality'.

Clause 205: "Harm" etc

804 This clause defines harm as physical or psychological harm. This could include physical injuries, serious anxiety and fear; longer-term conditions such as depression and stress; and medically recognised mental illnesses, both short-term and permanent.

805 It provides that harm can arise from the harmful nature of content, for example from grossly offensive, abusive or discriminatory content. It can also arise from the dissemination of content that is not by its nature harmful, for example the malicious sharing of personal information, or the way in which content is disseminated, for example one or many people repeatedly sending content to an individual.

806 It also makes provision to include indirect harm, where someone harms themself or another person as a result of content.

Clause 206: "Online safety functions" and "online safety matters"

807 This clause sets out the meaning of "online safety functions" and "online safety matters".

Clause 207: Interpretation: general

808 This clause sets out the meanings of various terms used in the Bill.

Clause 208: Index of defined terms

809 This clause lists those provisions which define or explain terms used in the Bill.

Final provisions

Clause 209: Financial provisions

810 This clause sets out the financial provisions for the Bill.

Clause 210: Extent

811 This clause provides that the Bill extends to England and Wales, Scotland and Northern Ireland, with the exception of the provisions set out in subsections (2)-(6). Further details are included in the extent section of these notes.

Clause 211: Commencement and transitional provision

812 This clause explains when the different provisions of the Bill will come into force.

Clause 212: Short title

813 This clause establishes the short title of this legislation, when enacted, as the Online Safety Act 2023.

Commencement

814 Clause 211 provides for the commencement of the provisions in this Bill.

815 Subsection (1) sets out the provisions that will come into force on the day the Bill receives royal assent.

816 Subsection (2) sets out that the remaining provisions of the Bill will come into force on a day set out in regulations by the Secretary of State, and subsection (3) sets out that different days may be appointed for different purposes. Subsection (4) sets out that regulations made under subsection (2) may not bring clause 186 (Repeal of Part 4B of the Communications Act) into force before the end of the period of six months that begins with the date that will be specified in regulations (under paragraph 8(1) of Schedule 3).

817 Subsection (5) sets out that the Secretary of State may by regulations make transitional or saving provisions in connection with the coming into force of any provision of this Bill. Subsection (6) sets out that the power to make regulations includes the power to make different provision for different purposes.

818 Subsection (7) sets out that any power to make regulations under this section is exercisable by statutory instrument.

Financial implications of the Bill

819 The Bill includes powers to allow OFCOM to charge fees to industry in order to allow them to become cost neutral to the exchequer. Operating costs incurred by OFCOM in carrying out their 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.

Parliamentary approval for financial costs or for charges imposed

820 A money resolution is required where a Bill gives rise to, or creates powers that could be used so as to give rise to, new charges on the public revenue (broadly speaking, new public expenditure).

821 This Bill requires a money resolution because the Bill confers new functions on OFCOM (for example, OFCOM's duties to carry out risk assessments under clause 89, or OFCOM's enforcement functions in Chapter 6 of Part 7). This will entail a significant increase in OFCOM's costs (which could potentially lead to increased expenditure under the Office of Communications Act 2002), and the Secretary of State will incur significant costs in implementing the Bill. The Bill is also likely to lead to increased expenditure under the Crime and Courts Act 2013 in relation to the National Crime Agency's functions in relation to reports about child sexual exploitation and abuse content: see Chapter 2 of Part 4 of the Bill.

822 This Bill also requires a ways and means resolution. Generally, a ways and means resolution is required where a Bill creates or confers power to create new charges on the people (broadly speaking, new taxation or similar charges). The Bill requires a ways and means resolution because it contains a power to charge fees to certain providers of internet services to cover the costs of OFCOM's new regulatory functions (see Part 6 of the Bill), and because the way that the fees will be charged means that some providers will be paying more than the costs attributable to them. The Bill also requires a paying-in resolution (which is included as a limb of the ways and means resolution) because it provides for penalties to be paid into the Consolidated Fund of the United Kingdom (see clause 182).

823 These motions were passed in the House of Commons on 19 April 2022.

Compatibility with the European Convention on Human Rights

824 Lord Parkinson of Whitley Bay has made the following statement under section 19(1)(a) of the Human Rights Act 1998:
"In my view the provisions of the Online Safety Bill are compatible with the Convention rights."

825 Issues arising as to the compatibility of the Bill with the Convention rights are dealt with in a separate memorandum. This was published separately on gov.uk on 17 March 2022.

Compatibility with the Environment Act 2021

826 Lord Parkinson of Whitley Bay is of the view that the Bill as introduced into the House of Lords does not contain provision which, if enacted, would be environmental law for the purposes of section 20 of the Environment Act 2021. Accordingly, no statement under that section has been made.

Related documents

827 The following documents are relevant to the Bill and can be read at the stated locations:

- Online Harms White Paper and Consultation
- Online Harms White Paper Initial Government Response
- Online Harms White Paper Full Government Response
- Draft Online Safety Bill
- Law Commission report
- Joint Committee report on the Draft Online Safety Bill
- Digital, Culture, Media and Sport Committee report

- Petitions Committee report on Online Abuse
- Online Safety Bill
- Impact assessment
- Delegated powers memorandum
- Government response to the Joint Committee report

Annex A – Territorial extent and application in the United Kingdom

Provision	England	Wales		Scotland		Northern Ireland	
	Extends to E & W and applies to England?	**Extends to E & W and applies to Wales?**	**Legislative Consent Motion process engaged?**	**Extends and applies to Scotland?**	**Legislative Consent Motion process engaged?**	**Extends and applies to Northern Ireland?**	**Legislative Consent Motion process engaged?**
Part 1: Introduction							
Clause 1	Yes	Yes	No	Yes	No	Yes	No
Part 2: Key Definitions							
Clauses 2 – 4	Yes	Yes	No	Yes	No	Yes	No
Part 3: Providers of regulated user-to-user services and regulated search services: duties of care							
Chapter 1: Introduction							
Clause 5	Yes	Yes	No	Yes	No	Yes	No
Chapter 2: Providers of user-to-user services: duties of care							
Clauses 6 – 19	Yes	Yes	No	Yes	No	Yes	No
Chapter 3: Providers of search services: duties of care							
Clauses 20 – 29	Yes	Yes	No	Yes	No	Yes	No
Chapter 4: Children's access assessments							
Clauses 30 – 32	Yes	Yes	No	Yes	No	Yes	No
Chapter 5: Duties about fraudulent advertising							
Clauses 33 – 35	Yes	Yes	No	Yes	No	Yes	No
Chapter 6: Codes of practice and guidance							
Clauses 36 – 48	Yes	Yes	No	Yes	No	Yes	No
Chapter 7: Interpretation of Part 3							

Clauses 49 – 56	Yes	Yes	No	Yes	No	Yes	No
Part 4: Other duties of providers of regulated user-to-user services and regulated search services							
Chapter 1: User identity verification							
Clauses 57 – 58	Yes	Yes	No	Yes	No	Yes	No
Chapter 2: Reporting child sexual exploitation and abuse content							
Clauses 59 – 63	Yes	Yes	No	Yes	No	Yes	No
Chapter 3: Terms of service: transparency, accountability, and freedom of expression							
Clauses 64 – 67	Yes	Yes	No	Yes	No	Yes	No
Chapter 4: Transparency reporting							
Clauses 68 – 69	Yes	Yes	No	Yes	No	Yes	No
Part 5: Duties of providers of regulated services: certain pornographic content							
Clauses 70 – 73	Yes	Yes	No	Yes	No	Yes	No
Part 6: Duties of providers of all regulated services: fees							
Clauses 74 – 81	Yes	Yes	No	Yes	No	Yes	No
Part 7: OFCOM's powers and duties in relation to regulated services							
Chapter 1: General duties							
Clauses 82 – 84	Yes	Yes	No	Yes	No	Yes	No
Chapter 2: Register of categories of regulated user-to-user services and regulated search services							
Clauses 85 – 88	Yes	Yes	No	Yes	No	Yes	No
Chapter 3: Risk assessments of regulated user-to-user services and regulated search services							
Clauses 89 – 90	Yes	Yes	No	Yes	No	Yes	No
Chapter 4: Information							
Clauses 91 – 109	Yes	Yes	No	Yes	No	Yes	No

Chapter 5: Regulated user-to-user services and regulated search services: notices to deal with terrorism content and CSEA content							
Clauses 110 – 117	Yes	Yes	No	Yes	No	Yes	No
Chapter 6: Enforcement powers							
Clauses 118 – 138	Yes	Yes	No	Yes	No	Yes	No
Chapter 7: Committees, research and reports							
Clauses 139 – 147	Yes	Yes	No	Yes	No	Yes	No
Part 8: Appeals and super-complaints							
Chapter 1: Appeals							
Clauses 148 – 149	Yes	Yes	No	Yes	No	Yes	No
Chapter 2: Super-complaints							
Clauses 150 – 152	Yes	Yes	No	Yes	No	Yes	No
Part 9: Secretary of State's functions in relation to regulated services							
Clauses 153 – 159	Yes	Yes	No	Yes	No	Yes	No
Part 10: Communications offences							
Clauses 160 - 163	Yes	Yes	Yes	No	No	No	No
Clause 164	Yes	Yes	Yes	No	No	Yes	No
Clause 165	Yes	Yes	No	Yes	No	Yes	No
Clause 166	Yes	Yes	No	No	No	Yes	No
Clause 167	Yes	Yes	No	No	No	No	No
Clause 168(1)	Yes	Yes	No	No	No	No	No
Clause 168(2)	Yes	Yes	No	No	No	Yes	Yes
Clause 169	Yes	Yes	No	Yes	No	Yes	No
Part 11: Supplementary and general							

Clauses 170 – 188	Yes	Yes	No	Yes	No	Yes	No
Clause 189	Yes	Yes	No	No	No	No	No
Clause 190(1) to (3)	Yes	Yes	No	No	No	No	No
Clause 190(4) to (6)	No	No	No	Yes	No	No	No
Clause 190(7) to (9)	No	No	No	No	No	Yes	No
Clauses 191 – 192	Yes	Yes	No	Yes	No	Yes	No
Clause 193(1) to (2)	Yes	No	No	No	No	No	No
Clause 193(3) to (4)	No	No	No	Yes	Yes	No	No
Clause 193(5) to (6)	No	Yes	Yes	No	No	No	No
Clause 193(7) to (9)	No	No	No	No	No	Yes	Yes
Clause 193(10)	Yes	Yes	No	Yes	No	Yes	No
Clause 194(1)	Yes	Yes	No	Yes	No	Yes	No
Clause 194(2)	No	No	No	Yes	Yes	No	No
Clause 194(3) to (6)	Yes	Yes	No	Yes	No	Yes	No
Clause 194(7)	Yes	No	No	Yes	Yes	No	No
Clause 194(8)	Yes	No	No	No	No	Yes	No
Clause 194(9)	Yes	Yes	No	Yes	No	Yes	No
Clause 195 - 197	Yes	Yes	No	Yes	No	Yes	No
Part 12: Interpretation and final provisions							
Clauses 198 - 212	Yes	Yes	No	Yes	No	Yes	No
Schedules							
Schedule 1: Exempt user-to-user and search services							
	Yes	Yes	No	Yes	No	Yes	No

Schedule 2: User-to-user services and search services that include regulated provider pornographic content							
	Yes	Yes	No	Yes	No	Yes	No
Schedule 3: Timing of providers' assessments							
	Yes	Yes	No	Yes	No	Yes	No
Schedule 4: Codes of practice under section 36: principles, objectives and content							
	Yes	Yes	No	Yes	No	Yes	No
Schedule 5: Terrorism offences							
	Yes	Yes	No	Yes	No	Yes	No
Schedule 6: Child sexual exploitation and abuse offences							
	Yes	Yes	No	Yes	No	Yes	No
Schedule 7: Priority offences							
	Yes	Yes	No	Yes	No	Yes	No
Schedule 8: Transparency reports by providers of Category 1 services, Category 2A services and Category 2B services							
	Yes	Yes	No	Yes	No	Yes	No
Schedule 9: Certain internet services not subject to duties relating to regulated provider pornographic content							
	Yes	Yes	No	Yes	No	Yes	No
Schedule 10: Recovery of OFCOM's initial costs							
	Yes	Yes	No	Yes	No	Yes	No
Schedule 11: Categories of regulated user-to-user services and regulated search services: regulations							
	Yes	Yes	No	Yes	No	Yes	No
Schedule 12: OFCOM's powers of entry, inspection and audit							
	Yes	Yes	No	Yes	No	Yes	No
Schedule 13: Penalties imposed by OFCOM under Chapter 6 of Part 7							
	Yes	Yes	No	Yes	No	Yes	No
Schedule 14: Amendments consequential on offences in Part 10 of this Act							

	Yes	Yes	No	Yes	No	Yes	No
Schedule 15: Liability of parent entities etc							
	Yes	Yes	No	Yes	No	Yes	No
Schedule 16: Amendments of Part 4B of the Communications Act							
	Yes	Yes	No	Yes	No	Yes	No
Schedule 17: Video-sharing platform services: transitional provision etc							
	Yes	Yes	No	Yes	No	Yes	No

Subject matter and legislative competence of devolved legislatures

828 Most of the provisions of the Bill extend to the whole of the United Kingdom and are reserved under the internet services reservation. The offences under Part 10 (communications offences) extend to England and Wales only, and the flashing images offences extend to England, Wales, and Northern Ireland only. Clauses 195(2) - (7) set out other exceptions as to the extent of the Bill.

829 There is a convention that Westminster will not normally legislate with regard to matters that are within the legislative competence of the Scottish Parliament, Senedd Cymru or the Northern Ireland Assembly without the consent of the legislature concerned.

830 As set out in the "Territorial extent and application section" above, elements of the legislation interact with devolved competencies, and for a small number of provisions the UK Government will need to seek legislative consent from the Devolved Administrations.

a. The Bill confers power on Ministers in Scotland and Wales and the relevant department in Northern Ireland to amend the list of exempt educational institutions included at Schedule 1.

b. The Bill also confers a power on Ministers in Scotland to amend the list of CSEA offences included at Part 2 of Schedule 6. The Government is seeking legislative consent where these powers have been conferred.

831 The Bill also includes new communications offences in Part 10 relating to false and threatening communications. These currently apply to England and Wales and the UK Government will seek legislative consent for the application to Wales, alongside consent for any further extension to the Devolved Administrations.

ONLINE SAFETY BILL

EXPLANATORY NOTES

These Explanatory Notes relate to the Online Safety Bill as brought from the House of Commons on 18 January 2023 (HL Bill 87).

Ordered by the House of Lords to be printed, 18 January 2023

PUBLISHED BY AUTHORITY OF THE **HOUSE OF LORDS**