HIGH COURT OF JUSTICE
11 Dec 2025
BUSINESS & PROPERTY COURTS OF ENGLAND & WALES
IL-2023-000082

IN THE HIGH COURT OF JUSTICE **Claim No IL-2023-000082**
BUSINESS AND PROPERTY COURTS OF ENGLAND AND WALES
INTELLECTUAL PROPERTY LIST (ChD)

Before: Mr Justice Meade
Dated: 10 December 2025

B E T W E E N :

SKY UK LIMITED

Applicant

- and -

(1) BRITISH TELECOMMUNICATIONS PLC
(2) EE LIMITED
(3) PLUSNET PLC
(4) TALKTALK TELECOM LIMITED
(5) VIRGIN MEDIA LIMITED

Respondents

ORDER (PUBLIC VERSION)

UPON the order of Meade J dated 1 November 2023 as varied by the Order of Meade J dated 12 November 2024 (the "**2024 Order**")

AND UPON the application of the Applicant by application notice dated 14 November 2025 to extend and vary the operation of the 2024 Order (the "**Application**")

AND UPON reading the documents recorded on the court file as having been read

AND UPON the court being satisfied on the evidence before it that the operators of the Target Servers (as defined in Confidential Schedule 2 to this Order) use the services of the Applicant and each of the Respondents to infringe the Applicant's copyrights in the United Kingdom and that it is appropriate and proportionate to extend the 2024 Order in the terms proposed

AND UPON the Court recording that the Respondents are not wrongdoers and have not themselves infringed the Applicant's copyrights

AND UPON the Respondents neither consenting to, nor opposing, the application but considering that it is appropriate for the Court to determine the proportionality of relief

AND UPON the Fourth Respondent indicating that implementation of this Order would be carried out on its behalf by TalkTalk Communications Limited (t/a Platform X Communications) ("**PXC**")

AND UPON PXC undertaking to the Applicant and to the Court to keep the contents of the confidential schedules to this Order confidential and not to share the same with any third party

AND UPON considering the application on paper

IT IS ORDERED THAT:

This order contains the following schedules:

Schedule 1 – The Sky Channels
Schedule 2 – Target Servers (Omitted)
Schedule 3 – Target Websites
Schedule 4 – Target Server Detection and Notification Criteria (Omitted)
Schedule 5 – Target Website Detection and Notification Criteria (Omitted)
Schedule 6 – Technical Means
Schedule 7 – Confidential Material

Disabling of access

1 The Applicant shall be authorised, and the Respondents shall be required, to block or attempt to block access to each of the following:

(a) in respect of the Target Servers (as defined in Confidential Schedule 2 of this Order and as may hereafter be varied), IP addresses which the Applicant or its appointed agents have notified to the Respondents in accordance with this Order, only during the times permitted by Confidential Schedule 4 of this Order (**"Dynamic Blocking"**); and

(b) in respect of the Target Websites (as defined in Schedule 3 of this Order and as may hereafter be varied), any Uniform Resource Locator ("**URL**") or Fully

Qualified Domain Name ("**FQDN**") which the Applicant or its appointed agents have notified to the Respondents in accordance with this Order at all times ("**Static Blocking**").

Dynamic Blocking

2 The Applicant or its appointed agents may during the times permitted by Confidential Schedule 4 of this Order (each a "**Blocking Window**") notify to the Respondents an IP address for Dynamic Blocking as a Target Server pursuant to paragraph 1(a) of this Order if:

(a) the Applicant or its appointed agents have detected that the IP address is being used during the applicable Monitoring Period:

(i) to communicate to the public linear audio-visual footage of one or more Sky Channels ("**Channel Footage**") without authorisation; or

(ii) in a manner that meets one or more of the detection conditions specified in Confidential Schedule 4 of this Order; and

(b) the Applicant or its appointed agents have concluded that at the time of detection the IP address satisfies the requirements of Confidential Schedule 4 of this Order.

3 At a time no later than the conclusion of each Blocking Window, the Applicant or its appointed agents shall give a notice to the Respondents in accordance with paragraph 7 of this Order to unblock all Target Servers that were previously notified in accordance with paragraph 2 of this Order. The Respondents shall use their best endeavours to ensure that such unblocking occurs as soon as reasonably practicable after any such notification is received.

Static Blocking

4 The Applicant or its appointed agents may at any time notify to the Respondents a URL or FQDN for Static Blocking as a Target Website pursuant to paragraph 1(b) of this Order if its sole or predominant purpose is to enable or facilitate access to a Target Website listed in Schedule 3 of this Order, or it meets the relevant

detection conditions for a Target Website specified in Confidential Schedule 5 of this Order.

5 The Applicant or its appointed agents shall, at least once every five business days, take steps to re-evaluate each of the Target Websites previously notified for blocking in accordance with paragraph 1(b) of this Order. If and insofar as any URL or FQDN for a Target Website is no longer eligible for notification under paragraph 1(b) at the time of such re-evaluation, the Applicant or its appointed agents shall promptly give a notice to the Respondents in accordance with paragraph 7 of this Order to unblock any Target Website that utilises that URL or FQDN. The Respondents shall use their best endeavours to ensure that such unblocking occurs as soon as reasonably practicable after any such notification is received (and in any event within ten business days of being notified).

Technical means

6 For the avoidance of any doubt, paragraphs 1, 3 and 5 of this Order are complied with by a Respondent if that Respondent uses the technical means set out in relation to that Respondent in Schedule 6 of this Order, or any alternative and equivalent (including replacement) technical means, provided that the Respondent gives notice to the Applicant of the change, and in respect of the customers identified in relation to that Respondent in Schedule 6 of this Order. In the case of the Applicant, the lawful authority granted pursuant to paragraph 1 of this Order includes use of the technical means set out in relation to the Applicant in Schedule 6 of this Order.

Notifications to the Respondents

7 Any notifications given by the Applicant or its appointed agents under paragraphs 2 or 4 of this Order must:

(a) be notified to the Respondents by means of:

(i) publishing a consolidated list of all the IP addresses of the Target Servers for Dynamic Blocking during the Monitoring Period, on a secure electronic platform to which each of the Respondents has been given access by arrangement with the Applicant or its appointed agents; and

(ii) an email containing all URLs or FQDNs of the Target Websites for Static Blocking; and

(b) be published to the said platform at least once during each Monitoring Period (in the case of the IP addresses for Dynamic Blocking) or provided by email (in the case of the list of URLs and FQDNs for Static Blocking), or in such manner as may be agreed with the Respondents; and

(c) be published in such a manner that they are accessible to all Respondents as close to simultaneously as is reasonably practicable.

8 Any notifications given by the Applicant or its appointed agents under paragraphs 3 and 5 of this Order must be notified to the Respondents by the same means as those specified in paragraph 7 of this Order and given by no later than midnight on the day following the day on which the obligation to send the notification arose.

Time for compliance

9 When blocking access to a Target Server or Target Website as part of either Dynamic or Static Blocking under paragraph 1 of this Order, the Respondents shall use their best endeavours to disable access to the relevant IP address, URL or FQDN as soon as practicable and subject to the limits of their networks and resources.

10 For the avoidance of any doubt:

(a) for a Respondent to comply with paragraph 9 of this Order it shall be sufficient for it to use the technical means set out in relation to that Respondent in Schedule 6 of this Order: (i) in the case of Dynamic Blocking taking place under paragraph 1(a) of this Order, at least twice during each Blocking Window; and (ii) in the case of Static Blocking taking place under paragraph 1(b) of this Order, within ten business days of being notified of a new URL or FQDN for blocking in accordance with paragraph 4 of this Order, or according to such other schedule as may be agreed between the relevant Respondent and the Applicant in writing;

(b) the Respondents are wholly reliant on the Applicant or its appointed agents accurately identifying the Target Servers and Target Websites to be blocked

under this Order. The Respondents have no obligation to verify whether such determination is correct.

Sunset clause

11 This Order shall cease to have effect at 23:59 on 25 November 2027, unless the Court orders otherwise. The Applicant has permission to apply on or before that date to extend the operation of this Order for a further period, and any such application shall be:

(a) supported by evidence and on notice to the Respondents;

(b) listed (if possible) before Mr Justice Meade; and

(c) determined on the papers, unless the Court directs otherwise.

Notifications to third parties

12 Where the Applicant or its appointed agents notify an IP address for Dynamic Blocking as a Target Server, or a URL or FQDN for Static Blocking as a Target Website, in accordance with paragraphs 2 or 4 of this Order:

(a) they must within a reasonable period of the first occasion when that IP address, URL or FQDN is notified (being no later than 7 days from the date of the notification) send to the hosting provider associated with the IP address, or to the operator of the Target Website (or, if no contact details are given for its operator, to the hosting provider associated with its URL or FQDN) an electronic notice which contains the following information:

(i) that access to the IP address, URL or FQDN has been blocked in the United Kingdom by court order;

(ii) the identity of the party who obtained this Order;

(iii) a link to an internet location from which the public version of this Order may be accessed; and

(iv) a statement that affected server operators have the right to apply to the Court to discharge or vary the Order;

(b) in the event that the operator of a Target Server or Target Website makes a representation to the Applicants or their agents to the effect that it is operating lawfully and provides details of a postal address at which it may be served with proceedings, the Applicant shall within 7 days of receiving notice from the operator of the Target Server or Target Website, either de-notify the Target Server or Target Website in accordance with paragraphs 3 and 5 of this Order or shall apply for directions in relation to its status as a Target Server or Target Website, such application to be on notice to the website operator;

(c) the Respondents are wholly reliant on the Applicant accurately identifying the URLs and FQDNs to be blocked under the terms of this Order, and the Respondents have no obligation to verify whether the Applicant's or its agents' determination is correct.

13 Within 10 working days of this Order being implemented by a Respondent, that Respondent shall take reasonable steps to publish a statement to its customers (identified in relation to it in Schedule 6) in electronic form which contains the following information:

(a) that access to a number of (unidentified) servers associated with infringing Channel Footage, and the Target Websites, has been blocked by court order;

(b) the identity of the party who obtained this Order; and

(c) a statement that affected users have the right to apply to the Court to discharge or vary the Order.

14 For the avoidance of doubt, the Respondents are not required to make the information in paragraph 12 of this Order available to their customers at the same time as blocking occurs.

Changes to Confidential Schedules 4 and 5

15 All parties have permission to apply in writing to vary the contents of Confidential Schedules 4 and 5, such application to be supported by evidence and on notice to all the other parties.

Suspension of blocking measures

16 A Respondent will not be in breach of this Order if it temporarily ceases to take the steps ordered in paragraph 1 (either in whole or in part) upon forming the reasonable view that suspension is necessary:

(a) in order to:

(i) correct or investigate over-blocking of material which is, or is reasonably suspected to be, caused by the steps taken pursuant to paragraph 1;

(ii) ensure the reliable operation of its Internet Watch Foundation blocking system, if it reasonably considers that such operation is otherwise likely to be impaired;

(iii) maintain the integrity of its internet service or the functioning of its blocking system;

(iv) upgrade, troubleshoot or maintain its blocking system; or

(v) avert or respond to an imminent security threat to its networks or systems;

(b) and provided that:

(i) it notifies the Applicant or its appointed agents of such suspension and the reasons for the same as soon as reasonably practicable; and

(ii) such suspension lasts no longer than is reasonably necessary.

Permission to apply

17 The following persons have permission to apply on notice to vary or discharge this Order insofar as it affects them, namely:

(a) The operator of any Target Server or Target Website which is notified under paragraphs 2 or 4 of this Order;

(b) The operator of any website or video streaming service who claims to be adversely affected by this Order;

(c) Any recipient of a notice under paragraph 12 of this Order; and

(d) Any customer of the Respondents who claims to be adversely affected by this Order.

18 Any application under paragraph 17 of this Order shall be on notice to all the parties and be supported by evidence justifying the grounds for the application, including a clear indication of the status of the applicant.

Confidentiality

19 In respect of the material identified in Schedule 7 of this Order ("**Confidential Material**"):

(a) Pursuant to CPR rule 31.22(2), the parties and their external advisors and experts may only make use of the Confidential Material for the purposes of these proceedings, whether or not they are read to or by the Court, referred to at the hearing of the Application or in skeleton arguments;

(b) Pursuant to CPR rule 32.13(2), the Confidential Material shall not be open to inspection; and

(c) The Confidential Material shall, if mentioned, be excluded from electronic and hard copy transcripts of the proceedings, save that nothing in this paragraph 19 shall prevent the Applicant from sharing Confidential Schedule 5 of this Order with third parties, on suitable terms as to confidentiality, for the purposes of securing its effective implementation or enforcement.

20 The Applicants shall be permitted to disclose details of each Blocking Window to any third party who has obtained or in future obtains an order under section 97A of the *Copyright, Designs and Patents Act 1988* or the Court's inherent jurisdiction for website blocking on a dynamic basis, or to the agents appointed by such a third party for the purposes of online enforcement.

Interpretation

21 In this Order:

(a) A reference to a "**Sky Channel**" is to be taken as a reference to an audio-visual stream which is broadcast on any of the satellite, cable or "over the top" technology, terrestrial and/or online channels identified in Schedule 1 of this Order (as may subsequently be varied or updated), including:

(i) any Standard Definition, High Definition, Ultra High Definition or other versions associated with each channel;

(ii) any catch-up or delayed broadcast versions of each channel; and

(iii) any changes to the name or format of those channels from time to time;

(b) A reference to a "**Monitoring Period**" or "**Blocking Window**" is to the corresponding period defined in Confidential Schedule 4 of this Order; and

(c) a reference to "**the Applicant or its appointed agents**" is to be taken as a reference to the Applicant, or its appointed agents for the purposes of online enforcement, including the third party mentioned in Confidential Schedule 4 or such other agent as may be appointed from time to time.

Other

22 The proceedings shall be stayed, save for the purposes of any application to give effect to the terms of this Order and save that the parties have permission to apply on notice in the event of any material change of circumstances including, for the avoidance of doubt but without limiting the generality of the foregoing, in respect of the costs, consequences for the parties and effectiveness of the aforesaid technical means from time to time.

23 The Applicant shall pay the Respondents their reasonable costs occasioned by this Order that relate to:

(a) the Respondents' marginal costs of the initial implementation of this Order insofar as such costs relate to Static Blocking only;

(b) the Respondents' marginal costs of complying with this Order during its lifetime insofar as those costs relate to Static Blocking only, including in response to notifications sent to the Respondents by the Applicant under paragraphs 4 and 5 of this Order.

24 Within 30 days of receipt by the Applicant of a Respondent written statement of the costs referred to in paragraph 23 of this Order, the Applicant shall pay to that Respondent those costs in full, unless within that period the Applicant disputes the claimed costs whether on the basis that those costs are unreasonable, or that they do not fall within paragraph 23 of this Order, or for any other reason.

25 The parties have liberty to apply in the event of any dispute as to the costs occasioned by this Order, including the costs payable under paragraphs 23 and 24 of this Order.

26 This Order shall be served by the Applicant upon (i) each of the Respondents and (ii) TalkTalk Communications Limited (for the sole purpose of it implementing the Order on behalf of the Fourth Respondent).

Service of the Order

The Court has provided a sealed copy of this order to the serving party:

Solicitors for the Applicant
DLA Piper UK LLP
160 Aldersgate Street
London EC1A 4HT
Ref: HC29/447836-2

Schedule 1: Sky Channels

The Sky Channels are:

Channel Name	EPG #	Type
Sky Showcase	106	Entertainment
Sky Witness	107	Entertainment
Sky Atlantic	108	Entertainment
Sky Max	113	Entertainment
Sky Comedy	114	Entertainment
Sky Documentaries	121	Documentaries
Sky Crime	122	Documentaries
Sky Nature	124	Documentaries
Sky Arts	130	Entertainment
Sky Sci-Fi	139	Entertainment
Challenge	145	Entertainment
Sky Mix HD	151	Entertainment
Sky Replay	152	Entertainment
Sky Showcase +1	206	Entertainment
Sky Witness +1	207	Entertainment
Sky Atlantic +1	208	Entertainment
Sky Crime +1	222	Documentaries
Sky Cinema Premiere	301	Movies
Sky Cinema Select	302	Movies
Sky Cinema Hits	303	Movies
Sky Cinema Greats	304	Movies
Sky Cinema Animation	305	Movies
Sky Cinema Family	306	Movies
Sky Cinema Action	307	Movies
Sky Cinema Comedy	308	Movies
Sky Cinema Thriller	309	Movies
Sky Cinema Drama	310	Movies
Sky Cinema Sci-Fi Horror	311	Movies
Movies24	325	Movies
Movies24+	326	Movies
Sky Sport Main Event	401	Sports
Sky Sports PL	402	Sports
Sky Sports Football	403	Sports
Sky Sports Cricket	404	Sports
Sky Sports Golf	405	Sports
Sky Sports F1	406	Sports
Sky Sports Tennis	407	Sports
Sky Sports Action	408	Sports
Sky Sports News	409	Sports

Sky Sports+	412	Sports
Sky Sports Mix	416	Sports
Sky Sports Box Office	491	Sports (PPV)
Sky News	501	News
Sky Kids	609	Kids

and include any variations to the above channels and any additional channel which is owned and broadcast by Sky UK Limited, as may be notified to the Respondents in accordance with this Order from time to time.

Confidential Schedule 2: Target Servers (Omitted)

Schedule 3: Target Websites

The Target Websites are:

1 The website and internet protocol television service “BunnyStream”;

2 The website and internet protocol television service “CatIPTV”;

3 The website and internet protocol television service “EnigmaStreams”;

4 The website and internet protocol television service “GenIPTV”;

5 The website and internet protocol television service “GoTVMix”;

6 The website and internet protocol television service “IPTVMAIN”;

7 The website and internet protocol television service “Fast IP.tv”;

8 The website and internet protocol television service “IP-TV.uk”;

9 The website and internet protocol television service “IPTV-King.co.uk”;

10 The website and internet protocol television service “IPTV Subscribe.uk”;

11 The website and internet protocol television service “IPTV-UK.digital”;

12 The website and internet protocol television service “Kemo IPTV.tv”;

13 The website and internet protocol television service “UK Channels.co.uk”;

14 The website and internet protocol television service “UKIPTV Media.co”;

15 The website and internet protocol television service “The Sky IPTV.shop”;

16 The website and internet protocol television service “Calmahub.live”;

17 The website and internet protocol television service "NetflyTV";

18 The website and internet protocol television service "NecroIPTV";

19 The website and internet protocol television service "Xtremehd-UK";

20 The website and internet protocol television service "Venex";

21 The website and internet protocol television service "OK-IPTV";

22 The website and internet protocol television service "IPTV Premium";

23 The website and internet protocol television service "Cheap IPTV";

24 The website and internet protocol television service "IPTV Express";

25 The website and internet protocol television service "Storm Media";

26 The website and internet protocol television service "IPTV Smarters";

27 The website and internet protocol television service "Get Max TV";

28 The website and internet protocol television service "British IPTV";

29 The website and internet protocol television service "iptvlondon.uk";

30 The website and internet protocol television service "B1gxtream";

31 The website and internet protocol television service "FireIPTV";

32 The website and internet protocol television service "Digital Planet";

33 The website and internet protocol television service "Fast IPTV UK";

34 The website and internet protocol television service "Flixtele";

35 The website and internet protocol television service "IPTV Fiesta";

36 The website and internet protocol television service "TVPig";

37 The website and internet protocol television service "IPTV Trends";

38 The website and internet protocol television service "IPTVore";

39 The website and internet protocol television service "skymediauk.com";

40 The website and internet protocol television service "FireTVHD.uk";

41 The website and internet protocol television service "4KIPTV";

42 The website and internet protocol television service "YourIPTV";

43 The website and internet protocol television service "PrivateIPTVAccess";

44 The website and internet protocol television service "IflexIPTV";

45 The website and internet protocol television service "IPTVUK Homes";

46 The website and internet protocol television service "ProxIPTV";

47 The website and internet protocol television service "SyncIPTV";

48 The website and internet protocol television service "TVBox";

49 The website and internet protocol television service "Strong8k";

50 The website and internet protocol television service "PPVIPTV"; and

51 The website and internet protocol television service "Tvleader.uk",

and include any changes to the name, URL and/or FQDN for these websites, and any further websites identified in accordance with Confidential Schedule 5, which are notified in writing by the Applicant or its appointed agents to the Respondents from time to time (together the "**Target Websites**" and each a "**Target Website**").

Confidential Schedule 4: Target Server Detection and Notification Criteria (Omitted)

Confidential Schedule 5: Target Website Detection and Notification Criteria (Omitted)

Schedule 6: Technical Means

In relation to the First Respondent (British Telecommunications plc)

Dynamic Blocking

1 In respect of its customers to whose internet service the system known as RedCard is applied, whether optionally or otherwise, the technical means are IP blocking.

2 For the avoidance of doubt, paragraphs 1(a) of the Order is complied with if the First Respondent uses RedCard or any subsequent system or measure that has equivalent relevant functionality.

Static Blocking

3 In respect of its customers to whose internet service is provided through its fixed line network, the service known as Cleanfeed is applied where specific IP addresses or unencrypted Uniform Resource Locators (URLs) are to be blocked. The technical means are:

(a) IP blocking at the core network level in respect of each and every IP address notified to the First Respondent for IP blocking in accordance with this Order; and

(b) IP address re-routing at the core network level in respect of each and every IP address notified to the First Respondent for re-routing in accordance with this Order; and

(c) DPI-based URL blocking utilising at least summary analysis in respect of each and every URL notified to the First Respondent in accordance with this Order.

4 In respect of its customers who use the First Respondent's Domain Name System ("DNS") servers, the technical means is DNS blocking in respect of each and every domain name or sub-domain notified to the First Respondent in accordance with this Order.

5 For the avoidance of doubt, paragraph 1(b) of the Order is complied with if the First Respondent uses the systems known as Cleanfeed (for the avoidance of doubt, this does not require the First Respondent to adopt DPI-based URL blocking utilising detailed analysis) and BT's DNS service or any subsequent system that has equivalent relevant functionality.

In relation to the Second Respondent (EE Limited)

Dynamic Blocking

6 In respect of its customers whose internet service is provided through its fixed line network currently known as EE Home line and mobile network (including its hosted Mobile Virtual Network Operators (MVNOs)), and to whose internet service the system known as RedCard applied, whether optionally or otherwise, the technical means are IP blocking.

7 For the avoidance of doubt, paragraph 1(a) of the Order is complied with if the Second Respondent uses the system known as RedCard or any subsequent system that has equivalent relevant functionality.

Static Blocking

8 In respect of its customers to whose internet service is provided through its fixed line and mobile network (including its hosted Mobile Virtual Network Operators (MVNOs)), the system known as Cleanfeed is applied whether optionally or otherwise, the technical means are:

(a) IP blocking in respect of each and every IP address notified to the Second Respondent for IP blocking in accordance with this Order; and

(b) IP address re-routing in respect of each and every IP address notified to the Second Respondent for re-routing in accordance with this Order; and

(c) DPI-based URL blocking utilising at least summary analysis in respect of each and every URL notified to the Second Respondent in accordance with this Order.

9 In respect of its customers who use the Second Respondent's DNS servers, the technical means is DNS blocking in respect of each and every domain name or sub-domain notified to the Second Respondent in accordance with this Order.

10 For the avoidance of doubt, paragraphs 1(b) of the Order is complied with if the Second Respondent uses the system known as Cleanfeed (for the avoidance of doubt, this does not require the Second Respondent to adopt DPI-based URL blocking utilising detailed analysis) and BT's DNS or any subsequent system that has equivalent relevant functionality.

In relation to the Third Respondent (Plusnet plc)

Dynamic Blocking

11 In respect of its customers to whose internet service the system known as RedCard is applied, whether optionally or otherwise, the technical means are IP blocking.

12 For the avoidance of doubt, paragraph 1(a) of the Order is complied with if the Third Respondent uses RedCard or any subsequent system or measure that has equivalent relevant functionality.

Static Blocking

13 In respect of its customers to whose internet service the system known as Cleanfeed is applied whether optionally or otherwise, the technical means are:

(a) IP blocking in respect of each and every IP address notified to the Third Respondent for IP blocking in accordance with this Order; and

(b) IP address re-routing in respect of each and every IP address notified to the Third Respondent for re-routing in accordance with this Order; and

(c) DPI-based URL blocking utilising at least summary analysis in respect of each and every URL notified to the Third Respondent in accordance with this Order.

14 In respect of its customers who use the Third Respondent's DNS servers, the technical means is DNS blocking in respect of each and every domain name or sub-domain notified to the Third Respondent in accordance with this Order.

15 For the avoidance of doubt, paragraphs 1(b) of the Order is complied with if the Third Respondent uses the systems known as Cleanfeed (for the avoidance of doubt, this does not require the Third Respondent to adopt DPI-based URL blocking utilising detailed analysis) and BT's DNS or any subsequent system that has equivalent relevant functionality.

In relation to the Applicant (Sky UK Ltd)

16 In respect of its customers to whose internet service the system known as Hawkeye is applied, whether optionally or otherwise, the technical means are IP blocking.

17 For the avoidance of doubt, the lawful authority conferred by paragraph 1 of the Order covers the use by the Applicant of the system known as Hawkeye or any subsequent system that has equivalent relevant functionality.

In relation to the Fourth Respondent (TalkTalk Telecom Ltd)

18 In respect of its customers:

(a) to whose internet access service the system known as StreamShield is applied, whether optionally or otherwise, the technical means is URL blocking in respect of each and every URL notified to the Fourth Respondent in accordance with this Order; or

(b) to whose internet access service the measure known as blackholing is applied, whether optionally or otherwise, the technical means are IP blocking in respect of each and every IP address notified to the Fourth Respondent for IP blocking in accordance with this Order, using the measure known as blackholing.

19 For the avoidance of doubt, paragraph 1 of the Order is complied with if the Fourth Respondent uses the systems known as StreamShield and blackholing or any

subsequent system or measure that has equivalent relevant functionality, up to an overall limit under all live s97A orders to which the Fourth Respondent is subject to of 10,000 simultaneous IP addresses.

In relation to the Fifth Respondent (Virgin Media Ltd)

20 In respect of its fixed-line residential and business retail broadband customers to whose internet access service the system known as Web Blocker 3 is applied, or to whose internet access the measure known as blackholing is applied, the technical means are IP blocking.

21 For the avoidance of doubt, paragraph 1 of the Order is complied with if the Fifth Respondent uses either the system known as Web Blocker 3 (or any subsequent system that has equivalent relevant functionality) or blackholing.

Schedule 7: Confidential Material

The Confidential Material is:

1. The material identified in paragraph 1 of the Order of Mrs Justice Joanna Smith DBE dated 1 April 2022 and which has been disclosed to the Applicant pursuant to that Order;

2. The matters identified as confidential by highlighting in paragraphs 7 to 19 of the witness statement of Jiajun Chen dated 25 May 2023 and Exhibits JC1 and JC2 thereto;

3. The matters identified as confidential by highlighting in paragraphs 4, 15, 19, 23.1, 23.3, 23.4, 23.5, 25, 26, 27, 35, 37, 39, 44, 46, 47, 48.1, and 55 of the witness statement of Matthew Hibbert dated 26 May 2023 and Exhibit MH1 thereto;

4. The expert reports filed on behalf of the Applicant and dated 26 May, 19 July 2023 and 10 November 2023, including in so far as they mention the name of the person making those statements, that person's employer, and all Exhibits thereto;

5. The matters identified as confidential by highlighting in paragraphs 4 - 12 of the witness statement of Jiajun Chen dated 10 November 2023;

6. The matters identified as confidential by highlighting in paragraphs 1, 5, 9, 12 – 20, 22 – 25 of the witness statement of Matthew Hibbert dated 10 November 2023 and Exhibits MH2 and MH3 thereto;

7. The expert report filed on behalf of the Applicant dated 31 October 2024, including insofar as it mentions the name of the person making that report, that person's employer, and all Exhibits thereto;

8. The witness statement of Jiajun Chen dated 23 October 2024 and Exhibits JC3 and JC4 thereto;

9. The matters identified by highlighting in the witness statement of Matthew Hibbert dated 31 October 2024 and Exhibits MH5 and MH6 thereto;

10. The matters identified as confidential by highlighting in paragraphs 10 and 12 to 30 of the witness statement of George Lawson dated 14 November 2025;

11. The witness statement of Jiajun Chen dated 30 October 2025 and Exhibit JC5;

12. The expert report filed on behalf of the Applicant dated 14 November 2025, including insofar as it mentions the name of the person making that report, that person's employer, and all Exhibits thereto;

13. Confidential Schedules 2, 4 and 5 of this Order; and

14. Skeleton arguments and other documents insofar as they refer to any of the above material.