

IN THE COURT OF APPEAL (CIVIL DIVISION)
ON APPEAL FROM THE UPPER TRIBUNAL
BETWEEN:

CLEARVIEW AI INC

Appellant

-and-

THE INFORMATION COMMISSIONER

Respondent

APPELLANT’S APPEAL SKELETON ARGUMENT

dated 14 January 2026

*References to paragraphs of the UT judgment are in the form UT/ *. For the FtT’s judgment, FtT/ *. For the witness statement of Mr Thomas Jackson Mulcaire, which was before the FtT, Mulcaire/ *.*

A. INTRODUCTION AND SUMMARY

1. This appeal is about the material and territorial scope of the General Data Protection Regulation, as it applied before IP Completion Day (the “**EU GDPR**”) and after IP Completion Day (the “**UK GDPR**”) (together, the “**Regulations**”). It concerns a facial-recognition-based internet search engine service which the Appellant (“**Clearview**”, a foreign, US company) offered to its clients in the period leading up to 18 May 2022 (the “**Service**”). All such clients were foreign governments or their contractors. As the FtT held, they all used the Service exclusively in furtherance of their core State criminal law enforcement and/or national security functions.
2. In summary, the Service operated as follows: a client would upload an image of a person of interest; through the use of proprietary technology, the Service would then match the face shown in that image with any images of that person’s face held within a database of images constructed by Clearview using images drawn from the public internet (the “**Database**”); the matching images would then be served to the client, together with the relevant webpage links and any associated metadata.
3. The evidence before the FtT confirmed that the Service had been used by Clearview’s clients to enable the identification of a wide array of criminals/suspected criminals and victims of crime, including: sexual predators and the child victims of such persons; murderers; international drug smugglers; thieves; individuals who stormed the US Congress in the US Capitol riots of 6 January 2021 and individuals accused of committing war crimes in Ukraine in the current Russia-Ukraine war, with one US prosecuting attorney stating that he could “give

hundreds of examples of children who were being sexually exploited or raped and were rescued solely because of Clearview”: Mulcaire/69(a).

4. On 18 May 2022, the Information Commissioner (the “**Commissioner**”) gave a Monetary Penalty Notice (“**MPN**”) and Enforcement Notice (“**EN**”) to Clearview in respect of the Service (together, the “**Notices**”). The Commissioner alleged that, by operating the Service, Clearview breached the data protection rights of millions of data subjects resident in the UK, contrary to the EU GDPR in the pre-Brexit period and thereafter the UK GDPR. Through the MPN and the EN, he sought to fine Clearview over £7.5 million, and compel Clearview to stop processing the data of all UK residents. As Clearview cannot practicably in most cases distinguish an image of a UK resident from an image of anyone else, Clearview’s position was (and is) that it could only comply with the EN order by shutting down the Service entirely.
5. Clearview appealed the Notices to the FtT. The FtT found that the Commissioner did not have jurisdiction to give them, because Clearview’s processing was outside the material scope of the EU GDPR and, for that reason, also outside the territorial scope of the UK GDPR. The Commissioner appealed to the Upper Tribunal (“**UT**”).
6. Overturning the FtT, the UT found, in a judgment dated 6 October 2025 (the “**Judgment**”) that the Commissioner did have jurisdiction to give the Notices, relying on Article 3(2)(b) of the Regulations. That Article provides, in summary, that, where a controller is not established in the EU/UK, its processing will still be within the territorial scope of the Regulations where (i) that processing is “*of personal data of data subjects who are in the [EU/UK]*” and (ii) it relates to “*the monitoring of [those data subjects] behaviour as far as their behaviour takes place within [the EU/UK]*”.
7. The UT found that Clearview’s processing was caught by that provision on two separate bases. First, the UT found that Clearview’s own processing, by means of compiling and maintaining the Database, itself amounted to the monitoring of UK data subjects’ behaviour in the UK and so was related to such monitoring (the “**Database Finding**”). Secondly, the UT found that Clearview’s clients used the Service to monitor the behaviour of UK data subjects in the UK, and Clearview’s own processing was relevantly “*related to*” that monitoring activity so as to fall within the scope of Article 3(2) (the “**Client-Centred Finding**”). The UT rejected the FtT’s conclusion that the fact that the Service was used exclusively in furtherance of foreign State criminal law and national security functions took Clearview’s processing outside the scope of EU law, and thus outside the material scope of the EU GDPR under Article 2(2)(a) thereof.
8. Clearview now appeals against the Judgment, with the permission of the UT. Clearview advances three grounds of appeal.

9. By **Ground 1**, Clearview contends that the Database Finding is based on an erroneous, overly broad interpretation of Article 3(2)(b). The data processing undertaken by Clearview in the context of the construction and maintenance of the Database is not behavioural monitoring for the purposes of Article 3(2)(b). Clearview's technology cannot even recognise or detect behaviour, still less can it analyse it. Clearview does not itself monitor anyone's behaviour.
10. By Grounds 2 and 3, Clearview challenges the legality of the Client-Centred Finding. Clearview need only succeed on one of these grounds to warrant that finding being overturned:
- (1) **Ground 2:** the Client-Centred Finding is wrong in law: (i) Article 3(2)(b) cannot capture processing that is related to behavioural monitoring by a third party. Rather, that provision is designed to capture processing where the processing and the behavioural monitoring are done by one and the same person; (ii) in any event, there has never been any evidence which could properly support the conclusion that any client has ever used Clearview to monitor any data subject's behaviour *in the UK*, which is what Article 3(2)(b) requires; and (iii) in any event, there is no justification for treating *all* of Clearview's processing of UK data subjects' data as within scope: at most, only the personal data of those UK data subjects whose behaviour in the UK had been monitored by Clearview's clients could be caught.
- (2) **Ground 3:** any behavioural monitoring undertaken by Clearview's clients, who are all foreign governments or their contractors performing governmental functions, would in any event be outside the scope of EU law and accordingly cannot, contrary to the Client-Centred Finding, act as the foundation for jurisdiction. "*Monitoring of [...] behaviour*" within the meaning of Article 3(2)(b) includes only monitoring that is itself subject to the Regulations. That is so, whether by dint of Article 2(2)(a) (which excludes from the scope of the EU GDPR any processing outside the scope of EU law) or general principles of EU/international law (which would prevent the EU from regulating the activities of foreign governments). It follows that any monitoring conducted by Clearview's clients cannot be "*monitoring of [...] behaviour*" covered by Article 3(2)(b). Indeed, in the eyes of the Regulations, there is no behavioural monitoring to which Clearview's processing can be said to be "*related*".

B. LEGAL FRAMEWORK

11. The material legislative provisions are set out below. It has always been common ground that the answer to the case would be the same, whether under the EU GDPR or the UK GDPR.

B.1 The EU GDPR

12. Article 2(1)-(2) of the EU GDPR (on **material scope**) provides as follows:

“(1) This Regulation applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.

(2) This Regulation does not apply to the processing of personal data:

(a) in the course of an activity which falls outside the scope of Union law [...].”

13. Article 3 of the GDPR (on **territorial scope**) provides as follows:

“(1) This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.

(2) This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:

(a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or

(b) the monitoring of their behaviour as far as their behaviour takes place within the Union.”

14. Recitals (23)-(24) of the GDPR address Article 3(2)(a) and 3(2)(b) respectively. They provide:

“(23) In order to ensure that natural persons are not deprived of the protection to which they are entitled under this Regulation, the processing of personal data of data subjects who are in the Union by a controller or a processor not established in the Union should be subject to this Regulation where the processing activities are related to offering goods or services to such data subjects irrespective of whether connected to a payment. In order to determine whether such a controller or processor is offering goods or services to data subjects who are in the Union, it should be ascertained whether it is apparent that the controller or processor envisages offering services to data subjects in one or more Member States in the Union. Whereas the mere accessibility of the controller's, processor's or an intermediary's website in the Union, of an email address or of other contact details, or the use of a language generally used in the third country where the controller is established, is insufficient to ascertain such intention, factors such as the use of a language or a currency generally used in one or more Member States with the possibility of ordering goods and services in that other language, or the mentioning of customers or users who are in the Union, may make it apparent that the controller envisages offering goods or services to data subjects in the Union.

(24) The processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union should also be subject to this Regulation when it is related to the monitoring of the behaviour of such data subjects in so far as their behaviour takes place within the Union. In order to determine whether a processing activity can be considered to monitor the behaviour of data subjects, it should be ascertained whether natural persons are tracked on the internet including potential subsequent use of personal data processing techniques which consist of profiling a natural person, particularly in order to take decisions concerning her or him or for analysing or predicting her or his personal preferences, behaviours and attitudes.”

B.2 The UK GDPR

15. Article 2 of the UK GDPR (the retained EU law version of the GDPR, and formally defined in s.3(10) DPA 2018), provides as follows:

“1. This Regulation applies to the automated or structured processing of personal data, including—

(a) processing in the course of an activity which, immediately before IP completion day, fell outside the scope of EU law [...].”

16. Article 3 of the UK GDPR provides:

“1. This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the United Kingdom, regardless of whether the processing takes place in the United Kingdom or not.

2. This Regulation applies to the relevant processing of personal data of data subjects who are in the United Kingdom by a controller or processor not established in the United Kingdom, where the processing activities are related to:

(a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the United Kingdom; or

(b) the monitoring of their behaviour as far as their behaviour takes place within the United Kingdom.

2A. In paragraph 2, “relevant processing of personal data” means processing to which this Regulation applies, other than processing described in Article 2(1)(a) or (b) or (1A).”

C. FACTS AND PROCEDURAL BACKGROUND

C1. The facts

17. Clearview is a Delaware corporation. At the relevant time, its headquarters were in New York, which was its principal place of business. (It has recently relocated to Texas.) It has no establishment or presence in the UK of any sort: FtT/22, Mulcaire/8-9. The case concerned the Service offered to Clearview’s clients (the “**Clients**”) over the period up to service of the Notices on 18 May 2022 (the “**Relevant Period**”).

18. Over the Relevant Period, the Service operated as follows (see FtT/42-43, and Mulcaire/10-31):

- (1) a Client would upload an image of an individual (typically a criminal suspect or a victim of crime) (the “**Probe Image**”), together with a case reference and investigation type;
- (2) Clearview would then derive a set of facial vectors from the Probe Image (a set of mathematical coordinates representing the Probe Image) (the “**Probe Vectors**”);
- (3) the Probe Vectors would then be cross-referenced with Clearview’s database of facial vectors (the “**Database Vectors**”), such vectors having been created by Clearview based on facial images which had (a) been published to the world at large on the internet and then (b) collected by Clearview by its web-crawlers;
- (4) where there was a match between the Probe Vectors and a particular Database Vector, the Service would display to the Client the images from which the relevant matching Database Vectors have been derived, together with the associated URL link to where the image

appears online and any associated metadata, that material having all been derived from the Database.

19. In effect, the Service operated much like a traditional internet search engine (“**TISE**”), except that whereas TISE searches are usually text-based, the searches on the Service were based on facial images. Moreover, and again like TISEs, Clearview stored the data in the Database in such a way as to make searches faster, known as ‘indexing’. Each facial vector was represented by a long list of numbers that represent coordinates in a coordinate plane. Vectors that derived from similar faces would have similar coordinates, nearer together in the coordinate plane, and therefore would be saved nearer to each other. This facilitated the efficient provision of search results: Mulcaire/29, FtT/28(f). The manner and location in which vectors were stored was in no way related to the behaviour of the person in the associated image, which Clearview’s technology cannot and does not detect.
20. The Service was (and is) designed to recognise faces. Clearview cannot rule out that users may use the results of searches in aid of behavioural monitoring activities, just as Clients may use TISEs to find out information about the people they are investigating or seeking to locate. However, any behavioural monitoring would necessarily be undertaken by a human Client and through their independent, separate, analysis of the search results they received: as above, the Service is incapable of recognising or detecting human behaviour. See the FtT’s (undisturbed) findings of fact to this effect at FtT/48, 50.
21. At all material times Clients of the Service had the following key characteristics:
 - (1) **Only foreign Clients.** The FtT found that the Service was “*not [...] used by clients in the UK nor in the EU*”, rather Clearview “*has clients in the United States of America and in other countries around the world including Panama, Brazil, Mexico, and the Dominican Republic*”: FtT/24.¹
 - (2) **Only State and State contractor Clients.** The FtT found that all Clients were “*government agencies or government agency contractors*” in those foreign jurisdictions: FtT/26(c).²

¹ Between June 2019 and March 2020, Clearview provided the Service to a small number of UK clients on a trial basis (the “**UK Trials**”): FtT/62. Only 721 searches were conducted in the course of the UK Trials. The UK Trials were historic when the Notices were issued some two years later. The Commissioner did not argue in submissions before the FtT that the UK Trials formed a basis for his jurisdiction, the FtT accordingly did not find any jurisdiction in relation to these searches and the UT dismissed the Commissioner’s argument that this was an error of law: see UT/321-323.

² It was apparent from the evidence before the FtT (which showed that 81% of Clients were police forces, FBI departments or military: Mulcaire/48) that no more than 19% of Clients could possibly have been contractors. In fact, the proportion of contractors was only 3%, though this figure did not need to be included because, as Mr Mulcaire explained at Mulcaire/49 and the FtT accepted at

- (3) **Only criminal law enforcement and national security Clients.** “All of [Clearview’s] clients carry out criminal law enforcement and/or national security functions, and use the Service in furtherance of those functions”: FtT/26(a) The FtT found that they were not permitted to use the Service for any commercial purpose: FtT/26(d). Clearview “does not provide the Service to any clients outside the criminal law enforcement/ national security context” (FtT/26(b)). See also FtT/146: “We have accepted Mr Mulcaire’s unchallenged evidence that all of CV’s current clients carry out criminal law enforcement and/or national security functions, and use the Service in furtherance of those functions”.

C2. The Notices

22. The Notices were given on 18 May 2022. By the MPN, the Commissioner sought to fine Clearview over £7.5 million in connection with its processing activities, specifically with respect to the processing of personal data of “UK residents”. By the EN, the Commissioner purported to require Clearview, in effect, to cease processing the data of all UK residents in the context of the Service. Apart from the conclusions on enforcement, the analysis in both Notices was materially identical. References below are to the MPN.

23. By the Notices, the Commissioner alleged that:

- (1) Clearview is the sole controller responsible for what is termed “*Activity 1 Processing*”, namely the creation, development and maintenance of the Database: MPN §§45-47.
- (2) This is distinguished from “*Activity 2 Processing*”, which encompasses Clearview’s receipt of the Probe Image from its Client, matching it against the Database, and then providing the applicable search results to the Client: §§48-49. For Activity 2 Processing, Clearview is a controller along with the relevant Client: §50.
- (3) Activity 1 Processing falls within Article 3(2)(b) of the Regulations. Clients seeking to match a Probe Image are monitoring the behaviour of the data subjects in the Probe Images, and in the images returned as a potential match. Clients “*may be able to ascertain information about a particular individual’s behaviour, not only at a particular point in time, but extending over a period of time*”. It is “*inevitable*” that a “*substantial number*” of those monitored in this way will be UK Residents. Clearview’s Activity 1 Processing is “*related to*” the monitoring carried out by its clients: MPN §§54, 56-57.
- (4) Activity 2 Processing falls within Article 3(2)(b) EU GDPR and UK GDPR. The location of the Client is not relevant. As above, matching a Probe Image against the Database

FtT/26(a), the factual position was no different for contractors and governmental authorities: all Clients were using the Service in furtherance of foreign State criminal law enforcement and/or national security functions.

constitutes monitoring the behaviour of UK Residents. Clearview’s Activity 2 Processing is “*related to*” the monitoring carried out by its Clients: MPN §§55, 58, 59.

24. Importantly:

- (1) There was no suggestion in the Notices that Clearview itself monitors the behaviour of any data subject. The only analysis advanced in the Notices was that Clients did so (the “**Client-Centred Case**”). Relatedly, there was no suggestion in the Notices that Activity 1 processing constituted the monitoring of behaviour, still less that the behaviour of all UK residents was being monitored. It was only (a) the individuals who appear in Probe Images, and (b) the individuals identified as a potential match in search results, that the Commissioner considered were being monitored.
- (2) The sole legal basis, in relation to both claimed Activities, on which Clearview was said by the Commissioner to be subject to Article 3(2)(b) was that its “*processing activities are related to*” the purported monitoring by Clearview’s Clients.
- (3) It was asserted without evidence or particularisation (save for mentions of the UK Trials) that a substantial number of UK data subjects would have their data processed in the context of both Activities, and that this involved monitoring their behaviour “*in the UK*”: §54(5).

C3. The FtT Decision

25. Clearview appealed the Notices, on both jurisdictional and substantive grounds. Jurisdiction was taken as a preliminary issue. By a late re-amendment to his pleading, the Commissioner began to advance a case absent from the Notices about ‘behavioural monitoring’ in light of Clearview’s evidence about indexing, now contending that Clearview was itself monitoring behaviour because Clearview “*sorts and organises images in the Clearview Database using their vectors before any Probe Image is submitted – and indeed irrespective of whether a Probe Image has been submitted – to enable more efficient use of computational resources and faster delivery of results*”: Commissioner’s Re-amended Response, §93 (the “**Indexing Case**”³).

26. In relation to jurisdiction, Clearview argued (in brief summary) that:

³ The Commissioner disavowed this characterisation of his alternative case in the UT, though the label was used by the Commissioner repeatedly at first instance (and appears in the FtT’s judgment). It is used for convenience here.

- (1) The Indexing Case was premised on a misreading of Article 3(2)(b). The organisation and indexing of facial vectors for efficient computation did not amount to, or convert database maintenance into, the “*monitoring of [...] behaviour*” within the meaning of Article 3(2)(b).
- (2) The Client-Centred Case advanced in the Notices also fell to be rejected, because: (i) Article 3(2)(b) only captures controllers who themselves monitor behaviour; (ii) in any event, even if that was wrong, Clearview’s processing was too remote from any behavioural monitoring that may be conducted by Clients to be “*related to*” such monitoring within the meaning of Article 3(2)(b); (iii) in any event, it had not been proven that any of Clearview’s clients had been monitoring the behaviour of UK residents in the UK; and (iv) in any event, even if there had been such monitoring and Clearview’s processing could be said to be “*related to*” it, any such monitoring was processing in the course of foreign governmental activities outside the scope of EU law, and thus excluded from the scope of the Regulations by Article 2(2)(a) EU GDPR. Monitoring that was outside the scope of the Regulations could not be the basis for establishing jurisdiction under the Regulations.

27. The FtT rejected the Commissioner’s new Indexing Case: FtT/129. Indexation was merely a processing operation to facilitate the efficiency of the Service. It did not rely on, use or reveal the behaviour of the data subject.

28. As to the Client-Centred Case advanced in the Notices, the FtT also found for Clearview:

- (1) The FtT accepted the Commissioner’s case that Clearview’s processing was “*related to*” Clients’ behavioural monitoring activities (FtT/138-144).
- (2) However, the FtT found that Clearview’s processing fell outside the material scope of the EU GDPR, and thus outside the scope of both Regulations. It noted that “*the activities of foreign governments fall outside the scope of Union law*” (FtT/123). Such were the activities of Clients: the FtT referred to the unchallenged evidence that the Service was only provided to non-UK/EU criminal law enforcement or national security bodies and their contractors, and held that all Clients used the Service in furtherance of criminal law enforcement and/or national security functions (FtT/146). The FtT held that “*it is not for one government to seek to bind or control the activities of another sovereign state*” (FtT/153), which was in substance what the Notices sought to do. In the premises, Clearview’s processing was “*in the course of an activity which immediately before IP completion day fell outside the scope of EU law*” (FtT/154) and outside the scope of the Regulations.

C4. The UT Decision

29. The Commissioner appealed with the permission of the UT. On appeal, Clearview advanced ‘Respondent’s Notice’ arguments to the effect that the Commissioner’s Client-Centred Case should also have been rejected because it was premised on misinterpretations of Article 3(2) of the Regulations, and because there was no proper basis for any finding that any relevant monitoring had ever taken place. The essential elements of the UT’s analysis of these issues (which are split across different parts of the judgment) are as follows:

(1) As to the Commissioner’s Indexing Case: the UT overturned the FtT, adopting what it called a “*broad interpretation*” of the words “*behavioural monitoring*”. See in particular UT/256-275, 306-320. This conclusion – referred to above as the Database Finding – is challenged by way of **Ground 1** in this appeal (summarised at §9 above).

(2) As to the Client-Centred Case,

- i. Affirming the FtT, the UT held that Clearview’s processing was “*related to*” Clients’ monitoring of data subjects’ behaviour in the UK. See UT/242-255, 325-330, 345-363. This is challenged through **Ground 2** in this appeal (summarised at §10(1) above).
- ii. Overturning the FtT, the UT held that Clearview’s processing was within the material scope of the EU GDPR, and so also constituted “*relevant*” processing for the purposes of UK GDPR. See UT/197-214 and 289-305. This is not challenged on this appeal.
- iii. However, the UT also rejected Clearview’s case, advanced at both levels below, that its processing was outside the scope of the Regulations because its Clients’ processing is outside the scope of EU law (and thus the material scope of the EU GDPR). See UT/331-344. That finding is challenged through **Ground 3** (summarised at §10(2) above).

D. GROUND 1: THE DATABASE FINDING

30. The UT erred in law by finding that Clearview’s own processing constitutes the “*monitoring of behaviour*” within the meaning of Article 3(2)(b), for the following reasons.

D.1 The presumption against extra-territorial effect governs the extent of extra-territorial effect, as well as its existence

31. There is a powerful presumption in domestic, international and EU law that legislation is not intended to have extra-territorial effect. Contrary to the UT’s findings, this governs the extent of extra-territorial effect of legislation, as well as the existence of such extra-territorial effect.

32. In domestic law, the presumption arises from a “*broad, general, universal principle that English legislation, unless the contrary is expressly enacted or so plainly implied as to make it the duty of an English*

Court to give effect to an English statute, is applicable only to English subjects or to foreigners who by coming into this country, whether for a long or a short time, have made themselves during that time subject to English jurisdiction”: **Re Sawers, ex p Blain** (1879) 12 Ch D 522, 526 approved in **Agassi v Robinson** [2006] 1 WLR 1380, HL at [16] and [20] *per* Lords Scott and Walker. There are important reasons of policy for that principle. It is “rooted” in “the concept of comity”, a “species of accommodation” which involves “mutual respect” between jurisdictions: **R (KBR) v Director of the Serious Fraud Office** [2022] AC 519. In that case, Lord Lloyd-Jones cited the definition given to comity by the US Supreme Court in **Hilton v Guyot** 159 US 113, 164 (1895), since cited by the Supreme Court of Canada, and extra-judicially by Judge Crawford (of the International Court of Justice): “Comity is the recognition which one nation allows within its territory to the legislative, executive or judicial acts of another nation, having due regard both to international duty and convenience, and to the rights of its own citizens or of other persons who are under the protection of its law.”

33. The presumption has particular force in relation to the acts of foreign persons located outside the UK. As Lord Rodger observed in **R (Al-Skeini) v Secretary of State for Defence** [2008] 1 AC 153 at [45], “[i]t would usually be both objectionable in terms of international comity and futile in practice for Parliament to assert its authority over the subjects of another sovereign who are not within the United Kingdom.” Further, because the presumption against extra-territorial effect has its roots in comity, “it is not necessary, in invoking the presumption, to demonstrate that the extra-territorial application of the legislation in issue would infringe the sovereignty of another State in violation of international law”: **KBR**, [25]. The presumption is “more extensive” than this and “reflects the usages of States acting out of mutual respect and, no doubt, the expectation of reciprocal advantage”.
34. In public international law, there is a “fundamental principle” of sovereign equality of states, recorded in Article 2(1) of the UN Charter, to the effect that one state’s sovereign legal order is equal to, and not to be subjected to, that of another. This principle “has to be viewed together with the principle that each State possesses sovereignty over its own territory and that there flows from that sovereignty the jurisdiction of the State over events and persons within that territory”: **Jurisdictional Immunities of the State (Germany v Italy; Greece intervening)** [2012] ICJ Rep 99, approved by the UK Supreme Court in **General Dynamics United Kingdom Ltd v Libya** [2022] AC 318 at [59].
35. In EU law, the same policy reasoning can be seen in the approach of the Court of Justice to extra-territorial effect, including in the field of data protection law. In Case C-507/17 **Google v CNIL** [2020] 1 WLR 1993, the Grand Chamber found that, though the Data Protection Directive required the operator of a search engine to de-reference sensitive information on the EU Member State versions of its search engine at the request of individuals, the Directive did not require a search operator to carry out worldwide de-referencing. This was because “the

balance between the right to privacy and the protection of personal data, on the one hand, and the freedom of information of internet users, on the other, is likely to vary significantly around the world”, and accordingly if it was not “*apparent from the wording*” ([60], [62]) of the Directive that the obligation was intended to extend to non-Member State versions of a search engine, it would be interpreted not to do so. A similar approach can be seen in Case C-366/10 ***Air Transport Association of America v Secretary of State for Energy and Climate Change*** (EU:C:2011:864). The claimants contended that the EU’s emissions trading scheme for aviation was enacted in excess of the EU’s powers because it was not confined to intra-European flights. The CJEU upheld the relevant directive, precisely because it took effect on a foreign aircraft operator only “*when its aircraft is in the territory of one of the Member States and, more specifically, on an aerodrome situated in such territory, since, in such a case, that aircraft is subject to the unlimited jurisdiction of that Member State and the European Union*”: [124]. It was because the flights that the scheme purported to regulate were physically over the territory of the EU that the scheme did “*not infringe the principle of territoriality or the sovereignty which the third States from or to which such flights are performed have over the airspace above their territory*”: [125].

36. The UT erred in its approach to the presumption. It analysed the Regulations on the basis that the presumption governs only the existence of extra-territorial effect, and not its extent: UT/159-160, 162(b), 170, 252. That is inconsistent with authority and principle:

- (1) It is contrary to the Supreme Court’s finding at [28] of ***KBR*** that “[t]he more exorbitant the jurisdiction, the more is likely to be required of the statutory provisions in order to rebut the presumption against extra-territorial effect.” The UT read that sentence as meaning that “*where there was exorbitance of the degree provided for in section 12 of the Bribery Act, express words were required to rebut the presumption against extra-territorial effect*”. That conclusion is wrong in law: the Supreme Court explicitly required the words of the statute to be measured against the extent of the extra-territorial effect, and there was no suggestion in the judgment of a simple binary question whether the exorbitance was sufficient to require express words or not.
- (2) The UT’s approach is also inconsistent with Lord Carswell’s speech in ***Al-Skeini***, in which he held at [97] that “*any extraterritorial jurisdiction of one state is **pro tanto** a diminution or invasion of the territorial jurisdiction of another, which must lead one to the conclusion that **such extraterritorial jurisdiction should be closely confined***” (emphasis added). It is unsurprising that the highest court approached matters in this way: as matter of logic, the binary approach risks exorbitant outcomes which jeopardise international comity.
- (3) The UT’s approach is also inconsistent with general principles of statutory construction. In the context of other interpretative presumptions, it has been specifically recognised that

the presumption does not cease to apply altogether simply because it is plain that some measure of effect against which the presumption operates was intended: see, in relation to the presumption against retrospective effect, *URS Corporation Ltd v BDW Trading Ltd* [2025] 2 WLR 1095 at [273] *per* Lords Hamblen and Burrows. To similar effect is the principle whereby statutes that interfere with rights and interests protected by the common law are presumed to do so only to a limited extent: see, for example, the approach in *R (UNISON) v Lord Chancellor* [2020] AC 869 at [88].

- (4) The UT further erred by suggesting at UT/162(a) (though without reaching any clear finding) that domestic authorities on the presumption against extra-territorial effect are not applicable to the Regulations. These authorities interpret and apply principles that are applicable to the construction of legislation enacted by any legislature with a geographically limited jurisdiction: contrary to the UT's suggestion at UT/162(a), it is not relevant that EU law is of a particular type of law distinct from that enacted by sovereign legislatures. The CJEU has in any event recognised the policy interests that underpin the presumption against extra-territorial effect, including in *Air Transport Association* and *Google v CNIL* above. The UT was wrong to dismiss the relevance of these authorities on the basis that the GDPR provides for some extra-territorial effect (see UT/164-170): they are relevant to ascertaining the extent of any extra-territorial effect.

D.2 Clearview's processing does not constitute the “*monitoring of behaviour*” within Article 3(2)(b)

37. It has never been alleged or found that Clearview undertakes any behavioural monitoring itself by servicing Clients' searches (i.e., by Activity 2 Processing). Nor could it be. Clearview does not, nor does its technology have the facility to, perform any operations on the search results to recognise, assess or analyse the behaviour of individuals. Compare the Court of Appeal's conclusion in *Soriano v Forensic News LLC* [2022] QB 533 that a journalist's investigative targeting of an individual's behaviour through extensive research about the individual's activities, assembling of that research and construction and publication of a story about the individual *arguably* amounted to behavioural monitoring within Article 3(2)(b). In the same case, Warby LJ expressly rejected as unarguable the characterisation of a published article describing the data subject's behaviour as being capable of being construed as 'monitoring': see [102].
38. Nor, on a proper analysis, does Clearview undertake any behavioural monitoring of its own by maintaining its database. The Commissioner correctly recognised this in the Notices under appeal in these proceedings, in which no such contention was advanced. The UT erred by making the Database Finding. The UT's conclusion, which extends the territorial scope of the

Regulations well beyond any previous authority, misconstrued Article 3(2)(b), and in particular the words “*monitoring of behaviour*”. The processing said to amount to behavioural monitoring is Clearview’s “*gathering, sorting and storing in a filing system organised person-by-person of ‘behaviourally rich’ data*”: UT/315. The reasoning that led the UT to its conclusion was infected by several errors of law, which together resulted in an overly-broad construction.

39. **First**, the UT was wrong to find that a controller can be engaged in behavioural monitoring where the controller neither recognises nor analyses (nor is capable of recognising or analysing) behaviour. As a matter of ordinary language, and *a fortiori* on the application of relevant canons of construction above, the monitoring of behaviour requires the ability to detect behaviour, and then the conduct of some analysis of that behaviour. That would include, most obviously, analysis of whether and, if so how, behaviour changes over time (“*monitoring*”). As the FtT recognised, Clearview cannot do any of that, and the UT rightly made no contrary finding.
40. The UT found that “*it is Clearview’s capability for identifying individuals that makes its Service such an ideal tool for behavioural monitoring*”: UT/269. Yet that goes nowhere on the issue of Clearview’s own activities. If Clients use the Service as a “*tool for behavioural monitoring*”, it may (depending on Ground 2 below) follow that those *Clients* are engaged in behavioural monitoring when using the Service. It does not logically follow that Clearview is itself engaged in behavioural monitoring. The UT was accordingly wrong to find, at UT/273, that Clearview is “*watchful*” if that word is stripped of its anthropomorphic connotations. Clearview cannot ‘watch’ behaviour even in a purely technological sense. The technology used by Clearview cannot recognise behaviour at all: its web crawlers and the tools used to construct the Database and deliver data to Service users do not and cannot distinguish between a headshot devoid of behavioural information, and, say, a picture of someone firing a gun. The technology is behaviourally blind.
41. **Secondly**, more generally, the UT confused Clearview’s own processing with that of its Clients. In particular, at UT/272, the UT observed that even before a Client uses the Service, “*Clearview has obtained and arranged information about an individual that would, or might, confirm details such as their name, the activities they undertake, both for work and leisure, whether they are married or in a relationship, whether they have children, and whether they have been arrested for, or convicted of, criminal offences*”. Again, this proposition had to be framed in the subjunctive mood (“*would, or might*”) precisely because nothing in Clearview’s own processing operations does in fact entail any detection, still less any ongoing watching of an individual’s activities, family life or criminal activity. The critical point is that the organising principle of Clearview’s processing is not behavioural identification or analysis, but facial similarity. Clearview’s Clients may be able to construct a picture of a person’s behaviour based, for example by systematic analysis of the data provided to them through use

of the Service, most obviously by combining it with other information in the Client's possession (i.e. other investigative information). However, Clearview cannot (and does not) construct such a picture through its own processing, because its own processing does not see behaviour or return results on that basis. The UT concluded that Clearview was behaviourally monitoring simply because the information it processed included information which, if analysed by others, may be capable of revealing behaviour. That is to ignore the 'monitoring' element of behavioural monitoring.

42. **Thirdly**, and relatedly, the UT erred in its reliance on Recital (24), insofar as it provides that "*it should be ascertained whether natural persons are tracked on the internet including potential subsequent use of personal data processing techniques which consist of profiling a natural person*". The UT relied on the reference to "*potential*" subsequent use of the data for its conclusion that the mere possibility of future monitoring activity by Clients suffices to make Clearview's own processing monitoring: see UT/265, 267, 275. Even on the UT's own analysis, Clearview's own processing is not the kind of processing contemplated by the Recital, namely processing "*including potential subsequent use*" of the data for profiling. That "*subsequent use*" is the Clients' subsequent use. Accordingly, the Recital does not provide any support for the UT's conclusion. The UT purports to make a finding on Clearview's own monitoring, but it collapses back into the finding that Clearview's processing is related to its Clients' monitoring.
43. **Fourthly**, the UT erred in its reliance on the Commissioner's analogy of a CCTV camera, which appears (see UT/266-267, 312) to have been the main basis for its conclusion that "*[t]he key to establishing monitoring is [...] that the data is available to be accessed should access be needed*". The UT appears thereby to have held that monitoring only need be possible or contemplated, to conclude that it has already occurred. That proposition is logically unsound as well as erroneous as a matter of construction, and the CCTV camera example provides no support for it. That the UT's reasoning results in a conclusion whereby every TISE (including e.g. the 'Wayback Machine') is engaged in behavioural monitoring of every data subject whose data it processes only underlines the surprising and incorrect nature of its conclusions.
44. **Fifthly**, the UT misconstrued and misapplied *Soriano*, in particular in its understanding of what type of processing the Court of Appeal considered to be arguable monitoring, as recorded at UT/265. The Court of Appeal in that case found that it was merely arguable that the controller was engaged in monitoring because they were collecting information "*about the behaviour in the EU of an individual*", then analysing "*that information*" (i.e., information about their behaviour) with a view to publishing an article "*about that behaviour*": see *Soriano*, [102]. Yet Clearview is not capable of recognising any behavioural information, still less analysing it. Compare the

activities of the journalists in **Soriano**, who reached multiple conclusions about the data subject's behaviour, such as that he "*is guilty of multiple homicide, has received illegal 'kickbacks', has been convicted of corruption in Monaco, is part of a money laundering operation and makes illegal arrangements for corrupt oligarchs and public figures*".

45. The UT erred, first, in that it understood the Court of Appeal to have "*decided*" that the Regulations apply to activities preparatory to publication of the information in question (see UT/104), whereas in fact Warby LJ was only identifying a case that he considered to be arguable. The UT further erred, at UT/310, in construing **Soriano** as establishing that the mere analysis, sorting and storage of data which happens to contain behavioural information can amount to monitoring, irrespective of whether the analysis in question is of human behaviours. The Court of Appeal established no such principle in **Soriano**. Quite the contrary, its analysis proceeds on the basis that the controller must conduct some form of behavioural analysis for there to be behavioural monitoring.
46. **Sixthly**, as well as erring in relation to "*behaviour*", the UT erred in relation to "*monitoring*". As a matter of ordinary language, the concept of "*monitoring*" requires analysis of whether and, if so how, behaviour changes over time (and/or, depending on context, through spatial position). Yet Clearview's technology does not enable, and is not capable of enabling, Clearview to determine whether (and if so how) a person's behaviour changes through space or time. In all the premises, the UT erred in finding that Clearview itself monitors behaviour.

E. GROUND 2: THE CLIENT-CENTRED FINDING AND ARTICLE 3(2)(b)

47. The UT upheld the Commissioner's case in the Notices that Clearview's processing was within the territorial scope of the Regulations because it was "*related to*" monitoring of the behaviour of UK data subjects in the UK/EU carried out by Clearview's Clients. That was in error of law, both because the UT failed to apply the presumption against extra-territorial effect when determining the extent of extra-territorial effect (see the points at Section D.1 above, which are repeated), and for the following additional reasons.

E.1 Clearview's processing cannot be 'related to' the monitoring of third parties within the meaning of Article 3(2)(b)

48. Article 3(2)(b) only captures the processing of controllers who are themselves engaged in behavioural monitoring. It does not capture the processing of controllers whose processing is related to the behavioural monitoring of a third party. That conclusion is strongly supported by the principle (set out above) that extra-territorial effect should be "*closely confined*" for reasons of

comity, and is in any event supported by a range of aids to construction, which were erroneously dismissed by the UT.

49. **First**, Clearview’s construction is strongly supported by the *travaux préparatoires*. In the European Commission’s proposal and impact assessment for the GDPR, accompanying the first draft text in January 2012, the Commission stated that the legislative intent of a regulation on data protection was to catch “*data controllers outside the EU if they offer goods and services (including information society services) to data subjects in the EU or monitor their behaviour*” (underline emphasis added, see UT/117). That suite of documents is the most direct and accurate indication of legislative intent available. That understanding of Article 3(2)(b) was maintained for the four years until the GDPR was enacted, as shown by the second document relied upon by Clearview in the UT, namely the European Commission Communication to the European Parliament and the Council in 2016 regarding Transatlantic Data Flows: Restoring Trust through Strong Safeguards, in which it was stated that “*the Regulation makes clear that it also applies to companies established in a third country if they are offering goods and services, or monitoring the behaviour of individuals, in the EU*” (emphasis added).
50. That understanding of the Regulations was also shared by the other EU institutions. On 11 April 2016, following interinstitutional negotiations, the European Commission commented that the Council of the EU (representing member states) “*confirm the Commission approach as regards the territorial scope of the Regulation which will also apply to controllers or processors established in a third country if they offer goods or services or monitor the behaviour of data subjects [sic] in the Union*” (see the Communication from the European Commission to the European Parliament pursuant to Article 294(6) TFEU, COM(2016) 214 final). The European Parliament voted on the Regulation on 14 April 2016, following a debate on 14 April 2016. At that debate, the European Parliament’s Rapporteur confirmed that there was now “*a consensus of all democratic parties in this House and of Member States in the Council*” and, though there was no explicit discussion of Article 3(2)(b), there was explicit discussion of Article 3(2)(a) where it was again confirmed that the ‘activities’ to be examined under Article 3(2) are those of the controllers, not third parties. The Member of the Commission in attendance told the Parliament: “*non-EU companies, when offering services in the EU, will have to abide by the same rules as EU companies*”. It was never suggested, in the course of those inter-institutional negotiations, that the understanding of Article 3(2) set out by the Commission when making its proposal, and agreed by the Council, was wrong.⁴

⁴ The *travaux* referred to in this paragraph were not before the UT, but are referred to here, for completeness.

51. The understanding of the legislative intent set forth in the Commission proposal was thus maintained for several years across institutions, representing a consistent understanding of the effect of Article 3(2)(b). At UT/235, the UT wrongly disregarded the *travaux* on the basis that the passages relied upon were “*brief*” and “*high level*”. The UT did not explain why the brevity of these statements reduced or undermined their reliability as a guide to legislative intent, and the UT erred in assuming that it did so.
52. **Secondly**, Clearview’s construction is strongly supported by Recital (24), which poses the question “*whether a processing activity can be considered to monitor the behaviour of data subjects*”. The recital thus envisages that, for the purposes of Article 3(2)(b), the person who carries out the relevant processing activity must themselves be conducting the monitoring to which the processing is said to relate. The part of that recital relied upon by Clearview is not addressed at all in the UT’s judgment, though the UT’s attention was expressly drawn to it.
53. **Thirdly**, Clearview’s construction is strongly supported by the words of Article 3(2)(a) and Recital (23). As was always common ground, Article 3(2)(a) is incapable of applying to processing “*related to*” a third party’s offer of goods and services. That conclusion is inescapable in light of Recital (23), which poses the question whether a controller “*is offering goods or services to data subjects who are in the Union*”. The words “*related to*” appear only once in Article 3(2), forming the stem of both Article 3(2)(a) and Article 3(2)(b). Yet the UT found at UT/246 that the words “*related to*” are nevertheless capable of denoting a relationship (a) that is confined to the activities of one person in Article 3(2)(a), and (b) that extends between the activities of two different persons in relation to Article 3(2)(b).
54. That transgresses the principle that “*when Parliament uses words in a statute those words should be given a similar meaning in other parts of the statute unless there is some reason to give them a different meaning*”: **R v Kansal (No. 2)** [2002] 2 AC 69, [102] *per* Lord Hutton. The UT did not explain how the words could thus have a “*consistent and coherent meaning*” across the two provisions when the UT has interpreted them to have a distinct effect, or how such an outcome is justifiable as a matter of principle or policy. That was a further error of construction and of logic.
55. In its analysis of this issue, the UT further misread [100] of **Soriano** (UT/253-254), reading Warby LJ’s judgment as supporting an “*expansive meaning*” of the words “*related to*”, because he approached the case on the basis that “*article 3(2)(a) applies to the processing of personal data of data subjects who are in the Union whether or not they are the same individuals as those to whom the goods or services are offered*” (**Soriano**, [100]). This passage of **Soriano** supports precisely the contrary view. Warby LJ was identifying a narrower reading (“*that the Regulation should apply to processing of an individual’s personal data that has some relationship with offering goods or services to that individual*”) that he plainly

considered to have force. He did not determine the point because it had not been argued. He was not endorsing the basis on which the case had been argued: if anything, he expressed scepticism about it. The UT also replicated its error regarding the European Data Protection Board (“EDPB”) Guidelines, applying passages of the Guidelines that deal with the position of processors, not controllers: UT/247-250, 255 (see below).

56. **Fourthly**, Clearview’s construction is supported by the EDPB Guidelines. These state: “*the use of the word “monitoring” implies that the controller has a specific purpose in mind for the collection and subsequent reuse of the relevant data about an individual’s behaviour within the EU*”. This envisages that the controller is itself doing the monitoring. The Guidelines further state: “*the fact of processing personal data of an individual in the Union alone is not sufficient to trigger the application of the GDPR to processing activities of a controller or processor not established in the Union. The element of “targeting” individuals in the EU, [...] by monitoring their behaviour (as further clarified below), must always be present in addition*”. Again, the EDPB’s view is that a controller must target EU data subjects “*by monitoring*” their behaviour to be caught by Article 3(2)(b).
57. The UT erred by relying on examples given in the EDPB Guidelines as to where a *processor’s* processing could be captured by Article 3(2)(b), where that processing was related to the monitoring activities of the *controller*. The UT assumed that, if a processor’s processing activities can be “*related to*” a controller’s monitoring within Article 3(2)(b), a controller’s processing activities can be “*related to*” a separate controller’s monitoring within that Article. The UT described the difference between the two scenarios as a mere “*factual difference*”: UT/240.
58. That was erroneous. The difference between processor and controller is, rather, an important *legal difference*. It is an organising principle of the Regulations that the legality of a processor’s processing will depend on matters determined by the controller: see, in particular, Article 29.⁵ It is the controller who decides the means and purposes of the processing (even where that processing is effected by a processor) and it is the controller who must ensure compliance of the processing (even where effected by a processor) with Articles 5(1)-(2) of the Regulations.
59. Accordingly, the question whether a *processor’s* processing relates to behavioural monitoring will depend on the activities of the controller. It cannot follow that the same should be true where the behavioural monitoring is conducted by a different controller. Hence, contrary to the UT’s analysis, it is not the inclusion of a ‘third party processor’ example in the EDBP Guidelines

⁵ “*The processor and any person acting under the authority of the controller or of the processor, who has access to personal data, shall not process those data except on instructions from the controller, unless required to do so by domestic law.*” (UK GDPR text)

regarding Article 3(2)(b) that is relevant to this case: it is the *absence* of a ‘third party controller’ example, which supports Clearview’s case.

60. In any event, the UT wrongly construed the Regulations on the basis that the EDPB Guidelines, a post-legislative aid that it (wrongly) considered to support the Commissioner’s construction, were of more assistance than the *travaux préparatoires*, a pre-legislative aid that supported Clearview’s. That was an error of principle and, to the extent that the UT suggested that it was supported by the Court of Appeal’s judgment in **Soriano** (at UT/237), that was wrong. The Court of Appeal did not have the benefit of any *travaux* in **Soriano** and did not consider their relevance.
61. **Fifthly**, Clearview’s construction is supported by the principles of legal certainty and foreseeability. Unless the controller caught by Article 3(2)(b) and the person undertaking behavioural monitoring are one and the same, then a controller’s subjection to the Regulations depends on the autonomous future decision-making of a third party that is not within the controller’s control and may well not be in the controller’s knowledge (as indeed is the case here). On that construction, a controller cannot foresee the obligations and penalties to which they may be subject as a result of their processing. That is too uncertain and unfair to have been the result intended by the legislature. Contrary to the UT’s statement at UT/176, it failed to construe the Regulations consistently with the principles of legal certainty or foreseeability (and in any event did not address the argument based on those principles regarding Article 3(2)(b)).
62. **Finally**, Clearview’s construction is supported by the principle that EU instruments should be consistently construed on all official EU languages. It is well-established “*that Community legislation is drafted in several languages, and that the different language versions are all equally authentic. An interpretation of a provision of Community law thus involves a comparison of the different language versions*”: **CILFIT Srl v Ministero della Sanità** (Case 283/81) [1982] ECR 3415, [18]. The English courts, including the appellate courts, often have regard to the official versions of EU instruments in other languages in the application of that principle: see e.g. **X v Mid Sussex Citizens Advice Bureau** [2013] ICR 249, [31]-[32] and [47]-[48] *per* Lord Mance. Accordingly, for the purposes of this appeal, Clearview commissioned brief advice from French, German, Italian, Spanish and Polish lawyers on whether it is possible in each official language, *purely as a matter of language and syntax*, to read Article 3(2)(b) as covering processing related to a third party’s monitoring activities. Either party’s construction is linguistically possible in French, Italian, Polish or German. However, notably, the response from Uria Menendez (a leading Spanish law firm) was:

“According to the Spanish version of Article 3.2(b) of the GDPR, the language presupposes that both the "processing" and the "monitoring" are done by the same entity (whereas as a data controller or processor). Spanish grammatical reading would not lead to understand the provision as applying to processing by one entity that is related to monitoring conducted by a different entity. The Spanish version establishes a single subject. The activities described in the Article are linked to a single grammatical subject, and the phrase "processing activities" (actividades de tratamiento) would refer to the processing by that subject. Therefore, the Spanish formulation assumes that the processing relates to the monitoring, which is carried out by one and the same entity.”

63. That provides further powerful support for Clearview’s construction: Article 3(2)(b) is aimed at processing through which the controller, itself, seeks to monitor the behaviour of UK/EU data subjects in the UK/EU. Any ‘behavioural monitoring’ activities of Clients are irrelevant.

E.2 No basis for the conclusion that any monitoring of any UK data subject’s behaviour in the UK has ever taken place

64. There has never been any evidence before the Commissioner or any tribunal that any Client has ever undertaken a search that returned any images of UK data subjects in the UK or EU. Nor has there ever been any evidence that any Client has ever undertaken a search using a probe image of a UK data subject. Still less is there any evidence that any Client has ever used the Service specifically in order to monitor the behaviour of a UK data subject in the UK.

65. The FtT concluded at FtT/140 that, *“on the basis of our factual findings [...] there is, more likely than not, monitoring of the behaviour of UK data subjects in the UK as far as their behaviour takes place in the UK”*. However, it did not identify those *“factual findings”*, and none of them supports the conclusion that any search of any UK data subject’s behaviour in the UK has ever been undertaken, or even that there has been a search of a UK data subject. The UT referred at UT/36 to *“the FTT’s findings about the nature and scale of the database, the international nature of crime, law enforcement and national security concerns, and the nature of Clearview’s clients’ activities”*.

66. However,

- (1) The nature and scale of the Database is logically irrelevant. However many images of UK data subjects appear on the Database, it does not follow that foreign Clients will have searched for UK data subjects; still less does it follow that foreign Clients will have searched for UK data subjects specifically in order to monitor their behaviour in the UK (as opposed to their behaviour in the local jurisdiction).
- (2) *“The international nature of crime, law enforcement and national security concerns”* is a plainly insufficient basis on which to conclude that, on the balance of probabilities, searches (or even a single search) of a UK data subject has in fact occurred. Still less is it a sufficient basis on which to conclude that, on the balance of probabilities, searches (or even a single search) of a UK data subject for the purposes of monitoring their behaviour in the UK

occurred. Even evidence to the effect that Clearview Clients had investigated UK data subjects would not be evidence that they had used Clearview to do so, and there was not even evidence of that kind. Nor even was there more general evidence about the extent to which agencies in the jurisdictions that Clearview serves investigate persons in the EU or UK. The fact that crime has international dimensions may entail a 0.1%, or 1%, or 10% chance that any Clearview Client has ever investigated a UK data subject using the Service: there is no explanation in the judgment of the FtT or UT for why it entails a probability of over 50%, and the UT did not explain how such an inference could possibly have been drawn. A theoretical possibility is not a fact proven on the balance of probabilities.

- (3) “*The nature of Clearview’s clients’ activities*” is that they use the Service in furtherance of their criminal law enforcement and/or national security functions. There has never been any evidence, nor any finding, that their activities include investigating any UK data subjects. Still less is there evidence that Clearview’s Clients were using the Service to investigate the behaviour of UK data subjects in the UK, as the terms of Article 3(2)(b) require.

67. Therefore, the Commissioner has not supplied any factual basis for his assertion of jurisdiction and the UT erred in apparently accepting that the assertion was made out.

E.3 In any event, the UT’s/Commissioner’s analysis could only extend to Activity 1 processing of UK data subjects whose behaviour in the UK is being monitored by Clients

68. If the Regulations applied to the Activity 1 processing at all (which they do not), they could only apply to that processing insofar as it concerns, specifically, processing by Clearview of data of those UK data subjects whose behaviour in the UK it is that Clearview’s Clients are seeking to monitor through their use of the Service. That construction is compelled by the words of Article 3(2)(b), which provides that the Regulations apply to the processing of data of “*data subjects who are in the United Kingdom [...] where the processing activities are related to the monitoring of their behaviour [...] within the United Kingdom*” (emphasis added). The Regulations do not say that processing of UK-located data subjects’ data is caught where it is related to the monitoring of some other UK-located data subjects’ behaviour or where it is related to the monitoring of behaviour outside of the UK: it must be related to the same (“*their*”) UK-located data subjects behaviour, and indeed be limited to where it is related to that same person’s behaviour in the UK.

69. The UT’s conclusions on this issue – namely, which Activity 1 processing by Clearview relates to behavioural monitoring of UK data subjects by its Clients – are, with respect, difficult to discern. However, to the extent that the UT found jurisdiction extending to other Activity 1 processing (for instance, of UK residents who have never been searched for, still less

successfully), that finding was in error of law. That is an important point, because Clearview has always maintained that, even if there have been searches of UK data subjects and indeed searches of UK data subjects' behaviour in the UK (as to which there is no evidence: see Section E.2 above), those searches would have been *de minimis*. They cannot be the foundation on which the Commissioner's jurisdiction over the entirety of Clearview's processing of data of UK data subjects is built. The Notices purport to regulate Clearview's processing of all UK residents' data, and must fall for that further reason.

F. GROUND 3: THE CLIENT-CENTRED FINDING AND ARTICLE 2/EU AND INTERNATIONAL LAW

70. Clearview's processing is outside the scope of the Regulations because its Clients' activities are excluded from the scope of the Regulations by Article 2(2)(a) GDPR and/or are otherwise excluded from the scope of EU law under general principles of EU or international law.

F.1 Article 3(2)(b) cannot apply to “*monitoring of behaviour*” that is outside the scope of EU law

71. Article 3(2)(b) cannot capture processing related to behavioural monitoring that is outside the scope of EU law. It is the behavioural monitoring referred to in Article 3(2)(b) that the legislature is seeking to regulate by that provision, as was common ground between the parties, and accepted by the UT: see UT/229-230, 241. Accordingly, Clearview's case, before the FtT and the UT, was that processing can only fall within Article 3(2)(b) of the Regulations where it relates to behavioural monitoring that is itself within the scope of EU law. Otherwise, the legislature would be seeking to regulate something it is not competent to regulate.
72. The UT rejected that case on the basis that, on its approach, the foreign State's processing is never brought within the scope of the Regulation, and only Clearview's processing is brought within scope: UT/341. This is form over substance. It is an exercise of a foreign State's sovereign authority how it decides to go about protecting its own essential State interests, such as the pursuit of criminal justice and the maintenance of national security, including a decision to pursue those interests by using Clearview's Service. Regulatory action by the Commissioner in respect of Clearview's Service necessarily interferes with that exercise of sovereign authority. The legislature cannot have intended such a result. As the FtT correctly found at FtT/153, “*it is not for one government to seek to bind or control the activities of another sovereign state*”. That is precisely what the Notices do: they seek to control the behavioural monitoring (if any such behavioural monitoring exists) conducted by foreign State criminal law enforcement and/or national security agencies.

73. The UT's analysis is artificial. In practice, it results in a situation where US police forces could readily use the Clearview Service if that service were operated 'in-house', but they cannot use it if it is operated by Clearview. The Notices have the effect of regulating how foreign States go about investigating crimes within their jurisdictions, albeit by the back-door. At UT/340, the UT had regard to its finding that Clearview's own processing is not outside the material scope of the Regulations on the application of Article 2(2)(d). That, however, was not relevant to the construction of Article 3(2)(b). The UT further reasoned that there is no express provision that 'behavioural monitoring' referred to in Article 3(2)(b) must be within the scope of EU law or the Regulation itself: UT/344. There did not need to be: what has already been excluded from the scope of the legislation need not be excluded again.
74. The UT further erred in law by holding that Article 2(2)(a) GDPR would not exclude from the material scope of the GDPR the activities of foreign States: UT/179-184, 186-196. It was common ground between Clearview and the Commissioner that the activities of foreign States fall outside the scope of EU law. The fact that previous cases concerning Article 2(2)(a) (and its predecessor provision in the Data Protection Directive) had concerned the division between EU competence and Member State competence, rather than the division between EU competence and foreign State competence, is irrelevant: the United States' national security activities are self-evidently outside the scope of EU law, whether or not France's are. However, in any event, the analysis is the same whether any behavioural monitoring activities by Clearview's Clients are excluded from the scope of the Regulations by Article 2(2)(a) (on material scope), as argued by Clearview and the Commissioner, or on wider principles of EU and/or international law (as accepted by the UT). Either way, Article 3(2)(b) cannot operate to regulate an activity that is outside the scope of EU law.

F.2 The UT erred by disturbing the FtT's finding of fact on the criminal law enforcement and national security activities of Clearview's state contractor Clients

75. The UT recorded at UT/281 that it was common ground that the processing of Clearview's foreign State Clients fell outside the scope of the Regulations. The FtT further made a finding of fact that Clearview's State contractor Clients carry out criminal law enforcement and/or national security functions, and use the Service in furtherance of those functions, based on the "*unchallenged evidence*" of Clearview's witness: see FtT/26. The Commissioner did not suggest before the UT that this evidence was challenged. It was not.
76. The UT found that the FtT's finding "*lacks specificity*" and that its primary findings of fact are inadequate to support its conclusion, so far as State contractors are concerned: UT/287. In fact, the FtT was well entitled to reach its findings about the nature of the activities of Clearview's

State contractor Clients, having regard to the evidence before it. This included evidence that Clearview’s Terms of Service prohibited users from “*using the service for a commercial purpose*” and that, in Clearview’s Code of Conduct, it was made clear that the Service is only for use by “*law enforcement and public security professional for legitimate law enforcement and public security purposes*”; and users “*shall not use the Clearview Platform for personal purposes, or for any purposes which are not authorized and directed by the Organization’s supervisors*”. Those terms were summarised at Mulcaire/49, and the FtT made express findings about them at FtT/26(d) of its decision, as it was entitled to do. The UT made no reference in its reasons to these more specific findings, and exceeded the limits of its appellate role by impugning the FtT’s findings of fact without any proper basis.

77. The UT also wrongly held that Clearview bore the burden of proving that all its Clients were out of the scope of the Regulations (UT/286). That misunderstands the Court of Appeal’s guidance in ***Doorstep Dispensaree Ltd v Information Commissioner*** [2025] 1 WLR 2635. Placing the legal burden of proof on an Appellant does not license the Commissioner to take regulatory action on a speculative basis, and then require an Appellant to disprove factual matters of which the Commissioner had to be satisfied to take such regulatory action. There is nothing in ***Doorstep*** to support any suggestion that the onus was on Clearview to lead individualised evidence about the activities in which each of its contractor Clients engaged over the Relevant Period, in order to respond to a speculative and entirely unevicenced suggestion from the Commissioner that contractor Clients may (contrary to the agreements Clearview put in evidence) have been using the Service for a commercial purpose. In any event, the approach to the burden could not affect the actual finding of fact made by the FtT, with which it was not for the UT to disagree.

G. DISPOSAL

78. The Court of Appeal is invited to set aside the Upper Tribunal’s decision, restoring the FtT’s decision that the Notices were outside the Commissioner’s jurisdiction.

ANYA PROOPS KC
CHRISTOPHER KNIGHT
RAPHAEL HOGARTH

11KBW

14 January 2026