



UA-2024-001563-GIA

Appeal No. UA-2024-001563-GIA
NCN [2025] UKUT 319 (AAC)

IN THE UPPER TRIBUNAL
ADMINISTRATIVE APPEALS CHAMBER

Between:

The Information Commissioner

Appellant

- v -

Clearview AI Incorporated

Respondent

- and-

Privacy International

Intervener

Before: **The Hon. Mrs Justice Heather Williams DBE**
Upper Tribunal Judge Church
Upper Tribunal Judge Butler

Decision date:
Decided after a hearing on: 9, 10 and 11 June 2025

Representation:

Appellant:	Mr Timothy Pitt-Payne KC and Mr Jamie Susskind, instructed by the Information Commissioner
Respondent:	Ms Anya Proops KC, Mr Christopher Knight and Mr Raphael Hogarth, instructed by Jenner & Block London LLP
Intervener:	Ms Marie Demetriou KC and Ms Aarushi Sahore, instructed by AWO

On appeal from:

Tribunal:	The First-tier Tribunal (General Regulatory Chamber)
Tribunal Case No:	EA/2022/0165/FP
Tribunal Venue:	Field House, London
Decision Date:	17 October 2023 (heard on 21 to 23 November 2022)

SUMMARY OF DECISION

INFORMATION RIGHTS (93)

This appeal is about the reach of data protection regulation under EU and UK law, and about whether the Information Commissioner had jurisdiction to issue an enforcement notice and a monetary penalty notice to the Respondent.

The Respondent is a US technology company which utilises 'crawlers' to 'scrape' the public-facing internet for images of human faces. When a facial image is identified, the image is collected (together with additional data), mapped using algorithms, assigned facial vectors, and stored in a searchable database that the Respondent maintains, comprising tens of billions of such mapped images. The Respondent's business involves selling access to its database to public and private sector clients operating in the fields of national security or criminal law enforcement. A client accesses the database by uploading a facial image to the Respondent's system, which initiates a search of the database for images with the same or similar facial vectors. A successful search results in the production of a report including images with facial vectors with a high degree of similarity to the vectors in the image uploaded by the client, together with other related data, that the client can use in furtherance of its national security or criminal law enforcement activities.

The appeal raises the issue of the extent to which processing of the personal data of UK data subjects by a private company based outside the UK is excluded from the scope of regulation, including where such processing is carried out in the context of its foreign clients' national security or criminal law enforcement activities.

The three-judge panel of the Upper Tribunal considered the proper interpretation of domestic and EU legislation (the UK General Data Protection Regulation ("GDPR") and the General Data Protection Regulation ("GDPR")), and decided that:

(1) the words "in the course of an activity which falls outside the scope of Union law" in Article 2(2)(a) of the GDPR (which provides for an exclusion from the material scope of the GDPR) refer only to those activities in respect of which Member States have reserved control to themselves and not conferred powers on the Union to act, and not to all matters without the competence of the Union (as the ICO argued) or to the activities of third parties whose processing "intersects" with their clients' processing in the course of "quintessentially state functions" which would offend against comity principles (as the Respondent argued);

(2) the words "behavioural monitoring" in Article 3(2)(b) GDPR are to be interpreted broadly, as a response to the challenges posed by 'Big Data' in the digital age, and they can encompass passive collection, sorting, classification and storing of data by automated means with a view to potential subsequent use, including use by another controller, of personal data processing techniques which consist of profiling a natural person.

"Behavioural monitoring" does not require an element of active "watchfulness" in the sense of human involvement; and

(3) the words "related to" in Article 3(2) of the GDPR, as applied to Article 3(2)(b), have an expansive meaning, and apply not only to controllers who themselves conduct behavioural monitoring, but also to controllers whose data processing is related to behavioural monitoring carried out by another controller.

The Upper Tribunal found that the First-tier Tribunal erred materially in law in finding that the Respondent's processing was outside the material scope of the GDPRs by operation of Article 2(2)(a).

The Upper Tribunal decided that the First-tier Tribunal was right to find that the Respondent's processing fell within the territorial scope of the GDPRs, albeit that it differed in its reasoning.

The Upper Tribunal allowed the appeal, set aside the decision of the First-tier Tribunal, and remitted the matter to the First-tier Tribunal to decide the substantive appeal on the basis that the Information Commissioner had jurisdiction to issue the notices.

Please note the Summary of Decision is included for the convenience of readers. It does not form part of the decision. The Decision and Reasons of the judges follow.

DECISION

The decision of the Upper Tribunal is to allow the appeal.

The decision of the First-tier Tribunal made on 17 October 2023 was materially in error of law. It is SET ASIDE under section 12(2)(a) of the Tribunals, Courts and Enforcement Act 2007 ("TCEA 2007") and REMITTED to the First-tier Tribunal under section 12(2)(b)(i) TCEA 2007 in accordance with the following Directions:

(1) The substantive appeal shall be listed for oral hearing before the First-tier Tribunal.
(2) Subject to what we say in [287] below, the findings of fact made by the First-tier Tribunal which heard the appeal on 21 to 23 November 2022 shall be preserved.
(3) The appeal shall proceed on the basis that the Information Commissioner had jurisdiction to issue the enforcement notice and the monetary penalty notice dated 18 May 2022 to the Respondent.

REASONS FOR DECISION

1. The structure of this decision is:

Introduction 5
What this appeal is about 5
The decision under appeal 5
A summary of the relevant factual background 6
The issues in this appeal 20
Appeal ground 1 20
Appeal ground 2 20
Appeal ground 3 21
Appeal ground 4 21
Additional Reason 1 21
Additional Reason 2 21
Additional Reason 3 21
Additional Reason 4 21
Preliminary matters 21
The scope of the appeal - admitting the additional reasons arguments for consideration 22
Permitting Privacy International to intervene in the appeal 22
Permitting Clearview to rely on a written reply to Privacy International's skeleton argument 23
Reliance on the evidence filed by Privacy International 23
Reliance on legal arguments not raised before the FTT 24
Legal framework 24
The Upper Tribunal's approach on an appeal against a FTT decision 24
Relevant legislative provisions 25
The Treaty on European Union 25
The GDPR 25
The UK GDPR 29
The 95 Directive 31
The Law Enforcement Directive 31
State immunity and foreign act of state 32
Material scope: the caselaw 34
Territorial scope: the caselaw 39
The Travaux in respect of the GDPR 42
The EDPB Guidelines 43
The burden of proof in appeals against ICO Notices 47
Analysis 48
Article 2(2)(a) GDPR: material scope 48
The parties' positions on material scope in brief 48
What the FTT decided in relation to Article 2(2)(a) 49
General approach to construction of the GDPRs 52
Domestic authorities on comity, extra-territoriality and utility 52
EU authorities on extra-territorial effect and comity 54
Certainty and foreseeability 56
Proportionality 57
EU law authorities on the construction of Article 2(2)(a) of the GDPR 57
Relevant comity principles 58
Our construction of Article 2(2)(a) 58
Analysis of Clearview's proposed intersectional construction 60
Alternative analysis based on the ICO's construction 63

Would regulation of Clearview's data processing breach comity principles? 63
Article 3(2)(b) GDPR: territorial scope....64
Our approach to the construction of Article 3(2)(b) 64
What was the policy objective behind Article 3(2)(b)?....66
The meaning of "related to" in Article 3(2)(b)....68
The meaning of "behavioural monitoring" in Article 3(2)(b) 70
The Grounds of Appeal 73
Ground 1....74
Ground 2....75
Ground 3....78
Ground 4....81
Clearview's Additional Reasons 81
Additional Reason 1 82
Additional Reason 2 82
Additional Reason 3 84
Additional Reason 4 86
Conclusion 87

Introduction

What this appeal is about

2. This appeal is about the reach of data protection regulation under EU and UK law. It is about the extent to which processing of the personal data of UK data subjects by a private company based outside the UK may be excluded from the scope of regulation, including where such processing is done in the context of its foreign clients' national security or criminal law enforcement activities.

3. We consider the proper interpretation of the domestic and EU legislation concerning data protection as well as the application of international law principles relating to comity between sovereign states.

The decision under appeal

4. The appeal concerns whether the UK Information Commissioner ("ICO") had jurisdiction under the General Data Protection Regulation ("GDPR") and the UK General Data Protection Regulation ("UK GDPR" and together with the GDPR, the "GDPRs") to issue an enforcement notice ("EN") dated 18 May 2022 and a monetary penalty notice ("MPN" and together with the EN, the "Notices") dated 18 May 2022 to the Respondent, Clearview AI Incorporated ("Clearview").

5. Because the appeal raises issues of special difficulty concerning the proper interpretation and application of the material scope provisions and the territorial scope provisions of the two GDPRs, a three-judge panel of the Upper Tribunal was convened to hear the appeal.

6. The ICO's appeal related to a substantive decision by the First-tier Tribunal (General Regulatory Chamber) ("FTT"), issued on 17 October 2023 that the ICO lacked jurisdiction to issue the Notices because Clearview's processing of personal data did not fall within the material scope of the two GDPRs.

A summary of the relevant factual background

7. The appeal arose from the Notices issued by the ICO following completion of his investigation into Clearview's activities in the UK. The Notices were issued on the basis that the ICO was satisfied that:

   (a) Clearview was a controller of data, as defined in sections 3(6) and 5 of the Data Protection Act 2018 ("DPA 2018"), Article 4(7) of the GDPR and Article 4(7) of the UK GDPR; and

   (b) Clearview's processing of the personal data of UK residents came within (and / or had previously come within) the scope of the GDPR (in relation to processing before 11pm on 31 December 2020) and the UK GDPR (in relation to subsequent processing), as a result of the application of Article 3(2)(b) of the GDPR and Article 3(2)(b) of the UK GDPR.

8. The ICO decided that Clearview had infringed Articles 5, 6, 9, 14, 15 to 17, 21 and 22 of the two GDPRs, and had failed to carry out a Data Protection Impact Assessment under Article 35. The ICO imposed a monetary penalty administrative fine on Clearview of £7,552,800 (equivalent to €9 million, using the exchange rate applicable at 25 April 2022).

9. Clearview appealed to the FTT on 29 June 2022. It challenged not only the identified breaches, but also whether the ICO had jurisdiction to issue the Notices. Clearview argued that, because it is a foreign company and because of the nature of the service it offered, and the clients to which it offered its service, it did not fall within the territorial scope of the GDPRs.

10. Clearview is an American technology company incorporated in Delaware. At the date of enforcement action taken by the ICO, Clearview did not have a corporate presence in the UK. The FTT found that when the ICO issued the Notices, Clearview had clients in the USA and other countries around the world including Panama, Brazil, Mexico, and the Dominican Republic.

11. The FTT described Clearview's principal service as supporting clients in the discharge of their criminal law enforcement / national security functions (with a view to assisting those clients in identifying criminal suspects / national security threats and the victims of crime) through the use of facial recognition technology that makes a comparison of an image submitted by the client against a database of images copied from the internet and saved by Clearview (the "Service").

12. Between June 2019 and March 2020, Clearview provided the Service to what it described as a small number of UK clients on a trial basis. The FTT referred to this in its decision as the "UK Test Phase", and found that during the UK Test Phase, 721 searches were made by UK clients.

The FTT's decision

13. The FTT held an oral hearing of the preliminary issue of whether the ICO had jurisdiction to issue the Notices under the GDPRs. That hearing took place from 21 to 23 November 2022.

14. The FTT issued its decision on the issue of jurisdiction nearly a year later, on 17 October 2023. The FTT acknowledged the substantial delay and apologised for the time it had taken to reduce its decision to writing.

The FTT's findings of fact

15. Having heard evidence given by Clearview's General Counsel, Mr Mulcaire, at the FTT hearing, the FTT made the following findings of fact about the Service:

> "28. The creation of the Database is, as described by the witness [Clearview's General Counsel], achieved by the:
>
> a. copying (which is often referred to as "scraping") of photographic images which have been published to the world at large on the public internet, i.e. without privacy controls being circumvented to copy the image;
>
> b. copying of additional information which relates to the photographic image such as a static URL[1], a link to the social media profile and the name of the profile if the image was sourced from a social media profile;
>
> c. the separation of those images that do not contain an image of a face from those containing images of faces (the former being discarded)[2];
>
> d. sending of the additional information to be stored in a proprietary database called SpeedyDB;
>
> e. creation of a set of vectors for each facial image using [Clearview]'s machine learning facial recognition algorithm;
>
> f. sending of the facial vectors to be stored in a database called Neural Network Data Base (NNDB). Vectors of faces that are similar to each other will be stored closer within the digital space than vectors of faces that are very different to each other. This clustering facilitates the efficient provision of search results to clients. The process of clustering similar vectors together was referred to as "indexing" during the proceedings;
>
> g. sending the Stored Image itself to be stored in a cloud database of images hosted by a third-party service provider;
>
> h. the retention of any image uploaded by a client in order to perform a search on the system (the "Probe Image") together with information that relates to the search such as its date and time. The Probe Images are not accessible to [Clearview] employees.

[1] A URL is the internet source of the image, the abbreviation stands for Uniform Resource Locator

[2] This process uses a face detection system similar to that on many mobile phones. It has been used by [Clearview] since 2022, prior to this the images that did not contain faces were identified and then retained albeit without facial vectors being created and without being used as part of the Service.

29. The scraping process uses automated programmes that visit publicly available websites and copy the images they find regardless of whether they contain an image of a face. These programmes are known as “scrapers” and the task of visiting websites as “crawling”. A scraper may be website-specific, that means it is specifically tailored to visit one website and copy the images from that one site more effectively. An open scraper will crawl numerous websites as it copies the images from each site. The [Clearview] open web scraper collects the most images, the website specific scrapers are not deployed at all times.

30. [Clearview] operates the open web crawler in-house but also uses contractors to provide scraped images.

31. Website-specific crawlers are used for sites that host a lot of images and are likely to be of interest to [Clearview]’s clients.

32. Websites may contain instructions within them that instruct web crawlers not to access them, such as robot.txt files. [Clearview]’s in-house open web crawlers will not scrape images from websites that have robot.txt files that do not authorise access by search engines. However, they also use results from external (outsourced) scrapers that are targeted at a single website; these scrapers do not abide by the instructions given by the robot.txt files. Such instruction will not prevent access without being accompanied by a preventative measure such as password protection.

33. Scrapers can be designed to evade privacy controls, such as those that protect some types of private social media accounts but scrapers used by [Clearview] are not programmed to do this. So, if a page is password protected, [Clearview]’s scrapers (both in-house and external) will not be able to access that page.

34. [Clearview] used to provide, to UK residents, a mechanism whereby a member of the public can request that their images are no longer used/stored by [Clearview] for the Service. This protection relied on positive action being taken by the member of the public.

35. [Clearview]’s web crawlers are prevented by their internal instructions from accessing tens of thousands[3] of adult websites. Neither do they copy content from some large social media platforms such as Snapchat and TikTok. This is because of technical reasons, for example certain social media platforms use a programming language called JavaScript which presents technical challenges.

36. A web crawler can be tasked to save the entirety of the web pages it visits. The web crawler used to compile traditional internet search engines or internet archives will do so, however [Clearview]’s scrapers copy only the image and additional information, not the entire page.

[3] The quantification is that given by Mr Mulcaire in answer to supplemental questions in evidence in chief.

37. The additional information that is collected with an image will depend on the source of the image and what has been attached to it. These pieces of additional information are forms of data collectively known as "metadata". [Clearview]'s scrapers will also collect the following types of metadata with each copied image:

a. a static URL, (the internet source of the image);

b. any text snippet that accompanies the image on its internet source page (e.g., the title of an image);

c. a link to the associated social media profile if the image was sourced from a social media profile;

d. the name of that profile and the text of the profile's description field;

e. any HTML meta element information which provides structured information about the source page;

f. any HTML "hover text" (also referred to as "hidden text") associated with the image that appears when a mouse cursor hovers over that image;

g. the file extension of the image file;

h. the Multipurpose Internet Mail Extension (or "MIME") of the image file (which indicates the nature and format of a document, file, or assortment of bytes);

i. a checksum hash of the image file (that is a digital data fingerprint of the image);

j. the image file's width, height and file size;

k. any available exchangeable image file data ("EXIF"), which may include camera-specific information, such as shutter speed, model details, flash settings, colour, space, date, and time.

38. [Clearview]'s scrapers only collect geolocation data, i.e. where a photograph was taken, if that image has retained the information within the EXIF data. This is because EXIF data is usually stripped away in the uploading process from the member of the public to the social media platform or other host site from which it is scraped. [Clearview] estimates that, in January 2022, 2% of the images on the database were accompanied by geolocation EXIF data based on a search of 3 billion images in the database. A previous estimate of 10% provided by the CEO in June 2020 was arrived at without such a search being carried out. It is also possible that a client can identify the location at which an image was taken from information stored in the webpage if they access the source of the image.

39. [Clearview] has the capacity to identify and block the utilisation of images taken in particular locations if such information is specified within the EXIF data of the image. The company can also place a "geo-fence" around a location to prevent the creation of facial vectors from any images scraped from that location as revealed in retained

EXIF data. Any such images are discarded after collection by the web crawlers. This is clear from the steps taken by [Clearview] after what was referred to as the "Illinois Settlement" of 4 May 2022 in which [Clearview] voluntarily:

a. Blocked all photos in the database that were geolocated in Illinois from being searched;

b. Constructed a 'geofence' around Illinois;

c. Decided that it will not collect facial vectors from images that contain metadata associated with Illinois; and

d. Decided that it will not collect facial vectors from images stored on servers that are displaying Illinois IP addresses or websites with URLs containing keywords such as "Chicago" or "Illinois".

40. [Clearview]'s Database contains billions of images. The size grows according to the number of images copied by the scrapers. In October 2022 it was estimated that the Database included over 20 billion images and increasing as new images are scraped. We were provided with an estimate of a growth rate of 75 million images per day.

41. Indexing is related to the value of the vectors created. Each facial vector is represented by a long list of numbers that represent coordinates in a coordinate plane which is the final output of a multi-layered algorithmic process. Vectors that derive from similar faces will have similar coordinates nearer together in the coordinate plane, and therefore will be saved nearer to each other. The database is not arranged to enable identification of a person's relatives or ethnicity. The algorithm focuses on what makes a person unique across different images and does not result in a significant family clustering effect. No index is kept of other objects in the Stored Image. The vectors created by [Clearview] are not transferable to another system, even though there are superficial similarities to software used to unlock phones or tablets and to other proprietary facial recognition systems. So, you could not take the vectors and input them to a phone or any other system to provide an image of the face in the photograph.

42. If one of [Clearview]'s clients wishes to use the Service, they will upload a facial image of an individual to [Clearview]'s system, this is known as a Probe Image. The system will create vectors for the face in the Probe Image. These vectors are then compared to the vectors created from the Stored Images using a machine learning facial recognition algorithm with a view to delivering a match or matches to the client. The results of that comparison are delivered to the client as search results that show the Probe Image alongside thumbnails of any Stored Images that the system has identified as having sufficient similarity to it. The number of results is capped at 120 for each search due to technical reasons.

> 43. The search results will include an assessment of the degree of similarity between each of the Stored Images returned by the search and the Probe Image, they will be presented in order of degree of similarity but no assessment of the accuracy of the matches is provided, the system does not indicate that the person in the Probe Image has been identified nor give a numerical percentage of confidence. The degree of similarity is represented by a coloured circle; a green circle indicates very close likeness between the vectors, whereas an amber circle would indicate a less strong likeness. The system does not say whether the images are of the same person, that decision is left to the client.
>
> 44. On a test by the US National Institute of Standards and Technology, a globally recognised test for facial recognition accuracy, [Clearview]'s service achieved 99%+ accuracy statistics. The algorithm is designed to require a high level of confidence before matching a Stored Image to Probe Image and returning it as a result of a search. Thus, it will not return the best match if the quality of the match is not high enough to satisfy that level of confidence, even if it is the best match from within the Stored Images. In those circumstances there will be no matches returned by the system.
>
> 45. The search results allow the client to select any of the thumbnails of the Stored Images. This will allow the client to see that image enlarged on screen together with the additional information including the URL. By using the URL the client may visit the internet page from which a Stored Image was copied/scraped.
>
> 46. The client will see three buttons in the search results for each image that when clicked on function as follows:
>
> a. "Download image" will download the image to the client's computer;
>
> b. "Copy site URL" will copy the URL into the client's clipboard so that they may enter it into another document/system;
>
> c. "Open site URL" will open that URL in a new internet tab."

The FTT's conclusions

16. The FTT concluded that the ICO did not have jurisdiction to issue the Notices because although the processing undertaken by Clearview was related to the monitoring of data subjects' behaviour in the United Kingdom, the processing was beyond the material scope of the GDPR and was not relevant processing for the purposes of Article 3 of the UK GDPR. See paragraph 1 of the FTT's Decision Notice.

17. To convey the FTT's reasoning on these issues, it is necessary to set it out in full:

> "111. We agree, and there was no dispute, that the images and additional information that are held in the [Clearview] Database constitute personal data. Vectors derived from images of a face would constitute special category data within the meaning of Article

4(14) GDPR and UK GDPR. Thus, not only does a Probe Image constitute personal data of the individual shown in that image, but the vectors derived from the face(s) shown in the Probe Image constitute special category data as they are biometric data falling within the definition in Article 4(14) to which Article 9(1) would apply.

112. [Clearview] are carrying out processing of personal data in the provision of the Service. The following functions are forms of that processing within the definition in Article 4(2), that are carried out to enable a client to search the [Clearview] Database to seek a match of a Probe Image against the Stored Images:

    a. scraping the images from the internet, this is collection;

    b. holding/storing the images;

    c. identifying those images which include a face and discarding images without a face;

    d. creating vectors from the stored images;

    e. creation/use of the blob ID;

    f. indexing/clustering of the stored images.

113. We find that c-f would be forms of organisation or structuring, adaptation or alteration, or retrieval and that all of the above forms of processing are encompassed in Activity 1 processing.

114. Activity 2 processing by [Clearview] includes the following types of processing that would fall within the definition provided in Article 4(2):

    a. upload of probe image to [Clearview];

    b. holding/storage of probe image;

    c. creation of vectors from probe image;

    d. matching of vectors of probe image against database of vectors;

    e. production of results;

    f. attachment via the use of the blob ID of the URL etc to the results;

    g. revelation of search results to client;

    h. attachment of an alert to the probe image;

    i. the client having uploaded their gallery of images, search of gallery images as against the [Clearview] database.

Behavioural monitoring

115. The heart of this case, in the Commissioner's submissions, is that the Service is being used to monitor the behaviour of data subjects. If we are not satisfied about that his case will fail, therefore we consider that aspect first.

116. It is necessary to decide what is meant by "behaviour" in this context because there is no definition. Every photographic image of a person will inevitably reveal something about them even, at the most basic level, that they had a photo taken or were standing up or were smiling, or simply that they were breathing, alive at the moment the photograph was taken.

117. It seems to us that the word *behaviour* indicates something more than simply being alive. We could not and do not purport to define everything that might come within the definition of behaviour. We consider that language is a tool that may be employed to determine (albeit not definitively) whether something is aptly described as *behaviour*. We have concluded that a description of a person's *behaviour* will include a verb. Such a description would reveal that the person is doing something, rather than the language solely communicating something about the person's characteristics. In other words *behaviour* goes beyond mere identification or descriptive terms such as the person's height hair colour, age, name or date of birth.

118. We are of the view that a person's behaviour would include:

    a. Where they are;

    b. What they are doing – including what they are saying/have said or what they have written as well as their employment or playing of a sport or their pastimes;

    c. Who they associate with in terms of relationships;

    d. What they are holding or carrying;

    e. What they are wearing – including any items indicating cultural or religious background or belief.

119. As set out above in our findings of fact the search results provided as examples to us revealed aspects of the behaviour of the individual(s) in the image including the person's:

    a. relationship status;

    b. parental status;

    c. associates;

    d. location or residence;

    e. use of social media;

    f. habits e.g. whether they smoke/drink alcohol;

    g. occupation or pastime(s);

    h. ability to drive a car;

    i. activity and whether that is legal and;

    j. whether the person has been arrested.

120. We also need to decide what "monitoring" means but once again we could not and do not purport to define everything that might come within the definition of monitoring as it will be intensely fact specific. We have had regard to Recital 24 and the need to ascertain whether natural persons are "tracked" on the internet including potential subsequent use of certain processing techniques which consist of profiling a natural person to take decisions about them; predicting or analysing, inter alia, their behaviour.

121. Thus, in the context of this case monitoring of a person's behaviour by a [Clearview] client using its Service could include:

    a. Establishing where a person is/was at a particular point in time;

    b. Watching an individual data subject over time by repeated submission of the same Probe Image of a known person;

    c. Using the matched images produced in response to a single search of a Probe Image to provide a narrative about the person in the images at the different times shown in those search results;

    d. Combining these results with information obtained from other forms of monitoring or surveillance.

122. These are all types of monitoring consistent with Recital 24 and in particular the reference to a person being "tracked" and thus monitoring will include a single incidence. It is important to note that the word is tracked as opposed to "tracking" which would imply a continuous or repeated activity. The verb "to track" is capable of bearing two meanings – the first being synonymous with hunting or searching for someone to establish their position at a fixed point in time and the second being the pursuit of a person over time, trailing them to identify where they are on more than one occasion.

123. We agree that the monitoring in this case is being done to identify a person but that is not the sole reason. [Clearview]'s clients use the Service to try to find out not only who a person is, but also with a view to taking decisions about them, predicting or analysing the person's behaviour in order to apprehend them/gather evidence about what they have done or to prevent illegal activity. We are satisfied that [Clearview]'s client organisations will use every piece of information they can gather to advance an investigation (that is their duty). Therefore, as in the example of the person who was located as a result of a search using [Clearview], the Service was used to glean information about where that person would be at a given time in order to apprehend them. That person was tracked on the internet and [Clearview]'s client took a decision about them, predicting their behaviour using the search results and any other information they had gathered to enable the person's apprehension.

124. The Commissioner's primary case is not that [Clearview] is monitoring the behaviour of data subjects but that its processing (in particular Activity 2 processing) is related to the monitoring of the behaviour of data subjects including those in the UK, through which the Commissioner's jurisdiction is said to be engaged.

125. The secondary case is that [Clearview] itself monitors behaviour, that is a view that was not relied upon in the notices, this is the "indexing case" which is dealt with later in this decision.

126. We have concluded that by using the [Clearview] Service as described above [Clearview]'s clients are "monitoring the behaviour" of those who appear in the Probe Images because they are seeking to identify facts about the individuals who appear in the Probe Images such as the examples given above, however the sole act of identification would not, in our view, be sufficient to constitute monitoring of the person's behaviour.

127. By considering the search results from the [Clearview] Database, and/or by considering those search results in conjunction with the Probe Image, or other information gathered as part of their investigation, [Clearview]'s clients may be able to ascertain information about a person's behaviour, either at a particular point of time, or extending over a period of time, however short that period. Obtaining or seeking to obtain information of this nature constitutes monitoring of the person's behaviour.

128. Reliance was placed by the Commissioner on the alert function within the Service. However, in our view the use of the alert function is not determinative of the existence of the monitoring of behaviour as the alert is given when the scrapers copy an image that matches the facial vectors of the Probe Image to which the alert has been attached. The scraped image may have been on the internet for some time and not copied into the system due to how the web crawlers function, thus the provision of the alert, of itself, tells the client nothing more than that the image has been found. However, if the alert is used to track the appearance of such images on the internet over time it could amount to monitoring of behaviour. This demonstrates the way the Service can be used by clients to monitor the behaviour of data subjects.

129. As to the indexing case, we find that this processing would not amount to the monitoring of behaviour. The Commissioner's case is that the activity of gathering the facial vectors created from personal data and indexing it according to the similarity in those vectors is comparable to a form of state surveillance and that [Clearview] is monitoring behaviour in this way. We find that the indexing case fails because the behaviour of a data subject is not used in the creation of the vectors or the indexing of the images according to those facial vectors. That processing in itself reveals nothing about the behaviour of a person because it is an automated, mathematical exercise. For this reason we conclude

that [Clearview] does not monitor the behaviour of data subjects in its own right. However, their processing of data when indexing facilitates the efficiency of the Service and as we conclude later is processing that is related to the monitoring of behaviour by [Clearview]'s clients.

130. As set out above there are four elements to be satisfied for the successful application of the criterion under Article 3(2)(b). We are satisfied that the first element is satisfied as there has been processing of personal data as described above, which was not in dispute.

131. We are further satisfied that the personal data that was subject to processing was that of data subjects in the UK and so we are satisfied about the second element. We conclude as set out in our factual conclusions above that the Database will include images of data subjects in the UK. We take the view that it is inevitable that the vectors from the UK data subject's images (personal biometric data) within the Database will be processed during the comparison of the Probe Image to the Database as part of the matching process. However, it is less likely that an image of a UK data subject will be produced as a successful match/partial match where the clients are investigating alleged crimes/threats within their jurisdiction (i.e. not within the UK). That is unless the UK data subject is an international criminal, has become involved in activity the subject of investigation, or the client is investigating a multinational threat.

132. The third element that must be satisfied is that the processing must be carried out by a controller or processor not established in the UK. As already stated it is agreed that [Clearview] is not established in the UK, neither are their clients, so far as the case is put to us by the parties.

133. As referred to above there are two types of processing activity relied upon by the Commissioner; Activity 1 processing, covering the creation, development and maintenance of the Database and Activity 2 processing, covering [Clearview]'s receipt of the Probe Image from the client, matching the Probe Image against the Database, and then providing the search results to the client.

134. A data controller determines the purposes and means of the processing of the processing of data, see Article 4(7).

135. [Clearview] is a controller of the data as regards Activity 1 processing. This was not in dispute.

136. We have concluded that [Clearview] is a joint data controller with their clients for Activity 2 processing. This is because:

    a. [Clearview] determines the purposes of the processing as it only provides the Service to those who wish to use it for purposes agreeable to [Clearview] within its terms and conditions, for

example not for any other purpose than matters of law enforcement and national security;

b. both [Clearview] and the client determine the means of processing; the client uploads the search image and [Clearview] conducts the matching process and provides the client with the matched images and additional information.

137. [Clearview] is also a processor for the purposes of both Activity 1 and Activity 2 processing.

138. We would add that even if we are wrong about our conclusions above about [Clearview] being a joint data controller nothing within the Regulation prevents the processing of data by a controller being related to the monitoring of behaviour by another distinct controller. This was the position in ***Soriano***. We agree with the Commissioner on this issue. We agree that the use of the words “the monitoring” as opposed to “their monitoring” indicates that the mischief is the monitoring and not who is doing the monitoring. If that were the case and Article 3 were restricted in the way contended for by [Clearview] this would mean that it would be a simple matter for a controller/processor to avoid Article 3 by dividing/delegating their processing and monitoring activities to different legal persons; “outsourcing” it as described by the Commissioner in order to avoid liability.

139. We are thus satisfied as to three of the four elements. The remaining common element is that the processing must be "*related to*" the monitoring of the behaviour of data subjects in the UK as far as their behaviour takes place within the UK.

140. So far as the second limb of the fourth element is concerned we have already concluded that there will be some images within the Database of UK data subjects taken within the UK and we have concluded that, although less likely, those images may be provided to clients as a search result. We have also concluded that [Clearview]’s clients may be investigating international activities. On the basis of our factual findings and having applied the law we have concluded that there is, more likely than not, monitoring of the behaviour of data subjects in the UK as far as their behaviour takes place within the UK.

141. Once again there is no definition of the phrase “*related to*” within the legislation or regulation(s). We respectfully agree with Warby LJ in ***Soriano*** that the phrase indicates that there must be a relationship between the processing of the individual’s personal data and the monitoring of behaviour that is in issue. The “compelling case” in ***Soriano*** was that information had been collected from the internet about a particular person and the data about that person had been assembled, analysed and ordered for the specific purpose of writing the article about that person’s behaviour which would be published. Publication was the processing that was complained about in the claim. The

preparatory activities of collation and analysis were integral to the publication of the article and Warby LJ held that it was arguable that the preparatory activities fell within the meaning of monitoring and were related to the publication given that was the purpose for which they were undertaken. We would observe that there was, in ***Soriano***, no other purpose for the collation, organisation and analysis of the data other than the publication. The whole purpose of the processing of data by [Clearview] is the provision of the Service to its Clients. There is no other purpose for the collation, organisation and analysis of the data in this case other than the use of that data by the clients using the Service.

142. [Clearview] is not simply processing the personal data in relation to one data subject as in ***Soriano***, but of millions if not billions of data subjects to facilitate the monitoring of behaviour by their clients.

143. There is such a close connection between the creation, maintenance and operation of the Database and the monitoring of behaviour undertaken by the clients that [Clearview]'s processing activities are related to that monitoring.

144. For all of these reasons we find that that [Clearview]'s processing is *related to* the monitoring carried out by the clients because:

a. Such monitoring by [Clearview]'s clients could not take place without [Clearview]'s Activity 1 processing;

b. The purpose of [Clearview]'s Activity 2 processing is to provide [Clearview]'s image matching service to its clients, thereby enabling the monitoring of behaviour carried out by [Clearview]'s clients to take place.

Was the processing in the course of an activity which falls/fell outside the scope of EU (Union) law?

145. We have not decided this case on the basis of a failure to meet the applicable burden of proof by either party. However, we observe (as have others before us in this Tribunal), that where a regulator issues a notice or imposes a penalty notice because of a breach of a regulation, and there is an appeal against the notice(s) there will be an initial evidential burden imposed upon the decision maker who is required to prove that the infringement has taken place. Where an appellant raises the issue of jurisdiction the Tribunal will need to be satisfied that there was power to issue the notices, i.e. that the decision under appeal/notices relate to acts or omissions to which the Regulations applied.

146. [Clearview] submits that, as a matter of fact, the Service is only provided to non-UK/EU law enforcement or national security bodies and their contractors. There was no evidence to the contrary tendered on behalf of the Commissioner. We have accepted Mr Mulcaire's unchallenged evidence that all of [Clearview]'s current clients carry out criminal law enforcement and/or national security

functions, and use the Service in furtherance of those functions, see above factual findings. That is the evidence placed before us by [Clearview] and while the Commissioner submits that there is an indication (in other words an inference) that any such contractors engaged by the clients are private sector bodies we are satisfied that any such contractors themselves carry out criminal law enforcement and/or national security functions. There is insufficient evidence on which to suggest otherwise.

147. The Commissioner is correct in submitting that the restriction upon who may use the Service only results from choices made by [Clearview] in how they offer the Service (at the time of the notices) and we agree that there is nothing that would prevent the Service being offered to commercial clients in the future but we are not satisfied that there is any present intention to do so. We conclude that the jurisdiction of the Commissioner to issue the notices falls to be decided on the Service at the time at which they were issued.

148. In any event we have concluded that [Clearview] does not monitor behaviour itself and it seems to us that Article 3(2)(b) is concerned with processing activities that are related to the monitoring of behaviour not processing activities that may be related to behavioural monitoring should there be a change of circumstances. Thus we reject the Commissioner's case that potential future processing brings the case within the material scope of the Regulations.

149. There is a specific directive applicable to law enforcement (Directive (EU) 2016/679 ("Law Enforcement Directive" / "LED")) which was not the subject of the case before the Tribunal. Action could be taken by the Commissioner pursuant to the Law Enforcement Directive (LED) against a UK established "competent authority" who used the Service were he to be of the opinion that such activity breached the LED. Whether or not in those circumstances [Clearview]'s processing would be beyond the material scope of the regulation is a distinct legal question that is not before us and does not assist us in deciding the issue that is before us which is based on other facts as we have found them.

150. The "Regulation" referred to in the opening words of Articles 2 and 3, and repeated within them is the GDPR/UK GDPR not the Article.

151. Article 3 GDPR is constructed such that if the criteria are satisfied the Regulation will be engaged and the remaining provisions applicable to the processing of the data concerned. Conversely Article 2(2) GDPR sets out types of processing to which the Regulation does not apply, excluding processing that would otherwise be caught by Article 3 from the application of the GDPR. In this case the relevant exemption that is relied upon is that processing was in the course of an activity which falls outside the scope of Union law.

152. As we have pointed out above (in paragraph 97) the UK GDPR is constructed differently and it is Article 3(2A) that removes processing in the course of an activity which fell outside the scope of Union law before IP completion day from the scope of the Regulation by excluding such processing from the definition of relevant processing in Article 3 UK GDPR.

153. Therefore, the question for us remains the same. It is foremost a question of fact as neither party contends that the acts of foreign governments would be within the material/territorial scope of the Regulations because the activities of foreign governments fall outside the scope of Union law. It is not for one government to seek to bind or control the activities of another sovereign state.

154. We have concluded, for all these reasons and on the basis of the unchallenged evidence, that [Clearview]'s processing was in the course of an activity which, immediately before IP completion day, fell outside the scope of EU law.

155. This is because Article 2(2)(a) GDPR operates to remove the processing with which we are concerned from the material scope of the Regulation in respect of the processing that took place before the exit of the UK from the European Union. So even though we have concluded that the terms of Article 3(2)(b) of GDPR brought the processing within the 'territorial' scope of the GDPR, the Regulation was disapplied to that processing as it was outside the material scope of the Regulation by virtue of Article 2(2)(a) GDPR for that processing that occurred before IP completion day.

156. Furthermore as regards the processing since that date, because the processing was in the course of an activity which, immediately before IP completion date, fell outside the scope of EU law that processing is not "relevant processing" of personal data as required by Article 3(2) UK GDPR and defined in Article 3(2A) UK GDPR. Thus, Article 3(2) UK GDPR does not apply to that processing and the processing that occurred after IP completion date is not within the scope of the Regulation as the material scope provision is disapplied.

157. Returning to the questions for us, we have concluded that:

    a. as a matter of law Art (3)(2)(b) can apply where the monitoring of behaviour is carried out by a third party rather than the data controller;

    b. as a matter of fact the processing of data by [Clearview] was related to the monitoring of behaviour by [Clearview]'s clients;

    c. the processing is outside material scope of the Regulation as provided for in Article 2 GDPR and is not "relevant processing" for the purposes of Article 3 UK GDPR, as defined in Article 3(2A) thereby removing the processing from the scope of UK GDPR."

The issues in this appeal

18. On 20 January 2025, Upper Tribunal Judge Wikeley granted the ICO permission to appeal on all the grounds set out in his application for permission to appeal.

19. The ICO advanced four numbered appeal grounds which may be summarised as follows.

Appeal ground 1

20. The FTT was wrong to hold that the behavioural monitoring carried out by Clearview's clients fell outside the scope of Union law.

21. The ICO argued two sub-grounds within this ground:

    Sub-ground 1: the FTT equated foreign Government bodies and the private sector contractors working for them; and

    Sub-ground 2: the FTT failed to distinguish between the activities of Clearview's private sector contractor clients that related to national security and those that related to law enforcement.

Appeal ground 2

22. Irrespective of what it decided about Clearview's clients, the FTT made an error of law in holding that Clearview's own processing fell outside the scope of Union law.

23. The ICO argued four sub-grounds within appeal ground 2:

    Sub-ground 1: the FTT failed to have regard to the fact the EN and MPN were directed at Clearview's own processing and not the processing by its clients;

    Sub-ground 2: the FTT failed to address Clearview's specific activities in the course of which its relevant processing took place (namely Activity 1 and Activity 2);

    Sub-ground 3: the FTT reached a conclusion that involved reading Article 2 and / or Article 3 of the GDPRs as if additional wording had been inserted into those provisions; and

    Sub-ground 4: the FTT reached a conclusion that would lead to an obvious anomaly and indeed absurdity in the application of Article 2(2)(d) GDPR but disregarded this when interpreting Article 2.

Appeal ground 3

24. The FTT was wrong to hold that Clearview itself did not carry out behavioural monitoring.

Appeal ground 4

25. The FTT was wrong in failing to consider whether the ICO had jurisdiction in relation to Clearview's activities during the UK Test Phase.

26. In its Response to the ICO's appeal to the Upper Tribunal, Clearview advanced four grounds upon which it invited the Upper Tribunal to uphold

the FTT's decision (to allow Clearview's appeal) for reasons additional to those provided by the FTT. Three of those grounds had been argued before the FTT but were rejected by it. One of them had been argued before the FTT but was not addressed in the FTT's decision. These grounds were described as Clearview's "Additional Reasons". They all relate to the FTT's decision that Clearview fell within the territorial scope of the GDPRs. Clearview argued that for the reasons it gave, and the additional reasons set out below, the FTT was right to find that the Notices exceeded the ICO's jurisdiction. Clearview's Additional Reasons may be summarised as follows.

Additional Reason 1

27. Article 3(2)(b) of the GDPR, which deals with territorial scope, is only capable of applying to a controller's processing where that processing is related to behavioural monitoring by that controller (as opposed to behavioural monitoring by a separate entity).

Additional Reason 2

28. In any event, Article 3(2)(b) is not engaged where the behavioural monitoring in issue is itself outside the material scope of the GDPR.

Additional Reason 3

29. Clearview's own processing would not be "related to" the monitoring of behaviour within the meaning of Article 3(2)(b).

Additional Reason 4

30. There was no evidence before the FTT of any processing of the data of UK data subjects related specifically to the monitoring of their behaviour in the UK / EU.

Preliminary matters

31. We dealt with a number of preliminary points in connection with this appeal, which we summarise below.

The scope of the appeal - admitting the additional reasons arguments for consideration

32. Clearview provided its Response to the ICO's appeal to the Upper Tribunal on 21 February 2025. Relying on rule 24(3) of the Tribunal Procedure (Upper Tribunal) Rules 2008 ("the UT Rules 2008"), Clearview raised its four Additional Reasons to support the conclusion that the ICO lacked jurisdiction to issue the Notices.

33. The ICO objected to Clearview being allowed to raise the Additional Reasons, on the basis that they effectively constituted a cross-appeal, and Clearview had not sought permission to cross-appeal within the relevant timescales.

34. In directions dated 30 March 2025, Upper Tribunal Judge Church, one of the three members of the three-judge Upper Tribunal panel, made case management directions that, in essence, treated Clearview as having sought permission to cross-appeal to the extent that such permission was needed,

extended time for the application, waived any irregularity in connection with the application and granted Clearview permission to raise the Additional Reasons arguments. Upper Tribunal Judge Church reasoned that there was a strong public interest in the Upper Tribunal considering the proper interpretation, and application, of Article 3 of the GDPR and the UK GDPR.

Permitting Privacy International to intervene in the appeal

35. On 25 April 2025, the Upper Tribunal received an application from Privacy International for permission to intervene in the proceedings to make submissions in support of some of the ICO's appeal grounds.

36. Upper Tribunal Judge Church allowed the application in a determination dated 16 May 2025 on the following bases:

    (a) rules 5(3)(d) and 33 of the UT Rules 2008 provide expressly for the Upper Tribunal to permit a person who is not a party to take specific steps in respect of an appeal (including making written and / or oral submissions), and the UT Rules 2008 do not prevent a person, who is not a party, intervening in proceedings before the Upper Tribunal with its permission;

    (b) the correct approach to apply towards an application to intervene was explained by Upper Tribunal Judge Wikeley in his determination of an application by a potential intervenor in ***Information Commissioner v Experian Limited*** (UA-2023-000512-GIA) at paragraphs 4-5;

    (c) the overriding objective favoured allowing Privacy International to intervene because the scope of the proceedings had been expanded to cover the issue of territorial jurisdiction. Upper Tribunal Judge Church was persuaded that Privacy International had special expertise and experience in this area which would complement, rather than duplicate, the ICO's expertise as the regulator of information rights in the UK and would be likely to assist the Upper Tribunal's understanding of the issues; and

    (d) the overriding objective also favoured allowing the intervention given the limited nature of Privacy International's proposed intervention, which was proportionate to the importance of the case, the complexity of the issues, the anticipated cost and the resources of the parties.

37. Upper Tribunal Judge Church therefore granted Privacy International permission to intervene, to make a written submission of no more than 25 pages, and to address the Upper Tribunal at the hearing (listed for 09 to 11 June 2025) for a period of 30 minutes or such other period the panel considered appropriate.

Permitting Clearview to rely on a written reply to Privacy International's skeleton argument

38. On 05 June 2025, Clearview filed a reply to the skeleton argument provided by Privacy International. In a letter dated 05 June 2025, the ICO objected to this, on the basis the submissions had been filed without permission, without forewarning and without explanation. It invited the Upper Tribunal to disregard the submissions as inadmissible, or (failing which) to reduce Clearview's time for oral submissions, to enable the other parties to address the new document.

39. At the hearing, the Chamber President, Mrs Justice Heather Williams, explained that we had read the relevant correspondence and the submissions from Clearview, that we regarded them as admissible, and we derived assistance from at least some of their contents. As the Chamber President observed, we considered it less of an ambush to the other parties for Clearview to have put these matters in writing, rather than simply set them out in oral submissions.

40. In our assessment, the written reply from Clearview clarified matters, not least because some of the arguments made by the ICO and Privacy International were conditional on whether Clearview was taking a specific position (which the ICO and Privacy International considered to be unclear). The reply from Clearview helped identify what remained in issue between the parties. We decided that admitting the written reply would best further the overriding objective in terms of dealing with the appeal in a way that was proportionate to the importance of the case and the complexity of the issues.

41. We accommodated the other parties' need to respond to the written reply. This included giving Privacy International an additional 10 minutes for oral submissions, as Ms Demetriou KC had requested.

Reliance on the evidence filed by Privacy International

42. At [23] to [26] of its reply to Privacy International's submissions, Clearview expressed a range of concerns about the Upper Tribunal placing reliance on three decisions regarding Clearview that were made by regulatory bodies in Greece, Austria and the Netherlands, that Privacy International had filed with its skeleton argument.

43. We dealt with this at the outset of the hearing by explaining that the Upper Tribunal was not a forum for introducing new factual issues or new factual evidence. We indicated that, to the extent that any party or intervener sought to raise new factual issues or rely on new factual material, that would not assist us, and we would not therefore admit it.

44. On that basis, we have not placed any reliance on any of the three regulatory decisions filed by Privacy International.

Reliance on legal arguments not raised before the FTT

45. As the Chamber President explained at the outset of the hearing, we decided to hear all the substantive submissions *de bene esse*, and to deal with the permissibility of those contentions being advanced (in so far as this was in issue), in our reserved judgment. In the event, we have had regard to all these submissions in arriving at our conclusions. In our assessment, the important nature of the issues we are asked to decide, including their novelty and their potentially wide-reaching implications, justifies permitting the parties to make fully reasoned submissions about these issues and having regard to those submissions in full in arriving at our decision. This approach best serves our inquisitorial role.

Legal framework

The Upper Tribunal's approach on an appeal against a FTT decision

46. The ICO brings his appeal under section 11 of the Tribunals, Courts and Enforcement Act 2007 ("TCEA 2007"). Section 12 of TCEA 2007 requires the Upper Tribunal to identify whether the making of the decision by the First-tier Tribunal in question concerned the making of an error on a point of law (section 12(1)). An error of law must be material for its setting aside to be warranted: see [9] to [10] of the Court of Appeal's decision in ***R (Iran) v SSHD*** [2005] EWCA Civ 982, which sets out a list of examples of the errors of law commonly encountered and explains that they incorporate a requirement of being "material".

47. The Upper Tribunal must exercise judicial restraint when examining the reasons given for a First-tier Tribunal's decision. The relevant principles were summarised at [64] to [65] of the decision of the three-judge panel of the Upper Tribunal in ***Information Commissioner v Experian Limited*** [2024] UKUT 105 (AAC):

> "64. As is well-known, the authorities counsel judicial "restraint" when the reasons that a tribunal gives for its decision are being examined. In *R (Jones) v FTT (Social Entitlement Chamber)* [2013] UKSC 19 at [25] Lord Hope observed that the appellate court should not assume too readily that the tribunal below misdirected itself just because it had not fully set out every step in its reasoning. Similarly, "the concern of the court ought to be substance not semantics": per Sir James Munby P in *Re F (Children)* at [23]. Lord Hope said this of an industrial tribunal's reasoning in *Shamoon v Chief Constable of the Royal Ulster Constabulary* [2003] UKHL 11 at [59]:
>
> " …It has also been recognised that a generous interpretation ought to be given to a tribunal's reasoning. It is to be expected, of course, that the decision will set out the facts. That is the raw material on which any review of its decision must be based. But the quality which is to be expected of its reasoning is not that to be expected of a High Court judge. Its reasoning ought to be explained, but the circumstances in which a tribunal works should be respected. The reasoning ought not to be subjected to an unduly critical analysis."
>
> 65. The reasons of the tribunal below must be considered as a whole. Furthermore, the appellate court should not limit itself to what is explicitly shown on the face of the decision; it should also have regard to that which is implicit in the decision. *R v Immigration Appeal Tribunal, ex parte Khan* [1983] QB 790 (per Lord Lane CJ at page 794) was cited by Floyd LJ in *UT (Sri Lanka) v SSHD* [2019] EWCA Civ 1095 at [27] as explaining that the issues which a tribunal decides and the basis on which the tribunal reaches its decision may be set out directly or by inference."

Relevant legislative provisions

The Treaty on European Union

48. Article 4 of the Treaty on European Union ("TEU") provides:

> **TITLE I**
>
> **COMMON PROVISIONS**
>
> *Article 4*
>
> 1. In accordance with Article 5, competences not conferred upon the Union in the Treaties remain with the Member States.
>
> 2. The Union shall respect the equality of Member States before the Treaties as well as their national identities, inherent in their fundamental structures, political and constitutional, inclusive of regional and local self-government. It shall respect their essential State functions, including ensuring the territorial integrity of the State, maintaining law and order and safeguarding national security. In particular, national security remains the sole responsibility of each Member State.
>
> 3. Pursuant to the principle of sincere cooperation, the Union and the Member States shall, in full mutual respect, assist each other in carrying out tasks which flow from the Treaties.
>
> The Member States shall take any appropriate measure, general or particular, to ensure fulfilment of the obligations arising out of the Treaties or resulting from the acts of the institutions of the Union.
>
> The Member States shall facilitate the achievement of the Union's tasks and refrain from any measure which could jeopardise the attainment of the Union's objectives.

The GDPR

49. Article 1 of the GDPR deals with its subject-matter and objectives. It provides:

> 1. This Regulation lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data.
>
> 2. This Regulation protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data.
>
> 3. The free movement of personal data within the Union shall be neither restricted nor prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data.

50. Article 2 deals with the material scope of the GDPR. We are particularly concerned with Article 2(2)(a) in this appeal. Article 2(1) and (2) provide:

> 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;
>
> (b) by the Member States when carrying out activities which fall within the scope of Chapter 2 of Title V of the TEU;
>
> (c) by a natural person in the course of a purely personal or household activity;
>
> (d) by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.

51. Article 3 deals with territorial scope of the GDPR. We are particularly concerned with Article 3(2)(b) in this appeal. Article 3 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 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.
>
> 3. This Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where Member State law applies by virtue of public international law.

52. Article 4 provides definitions within the GDPR. The definition of the word “profiling” is relevant. It provides:

> “profiling’ means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person’s performance at work, economic situation, personal preferences, interests, reliability, behaviour, location or movements.

53. A number of the Recitals to the GDPR are relevant to the issues before us. These recitals are:

> Recital 6: Rapid technological developments and globalisation have brought new challenges for the protection of personal data. The scale of the collection and sharing of personal data has increased significantly. Technology allows both private companies and public authorities to make use of personal data on an unprecedented scale in order to pursue their activities. Natural persons increasingly make personal information available publicly and globally. Technology has transformed both the economy and social life, and should further facilitate the free flow of personal data within the Union and the transfer to third countries and international organisations, while ensuring a high level of the protection of personal data.
>
> Recital 7: Those developments require a strong and more coherent data protection framework in the Union, backed by strong enforcement, given the importance of creating the trust that will allow the digital economy to develop across the internal market. Natural persons should have control of their own personal data. Legal and practical certainty for natural persons, economic operators and public authorities should be enhanced.
>
> Recital 15: In order to prevent creating a serious risk of circumvention, the protection of natural persons should be technologically neutral and should not depend on the techniques used. The protection of natural persons should apply to the processing of personal data by automated means, as well as to manual processing, if the personal data are contained or are intended to be contained in a filing system. Files or sets of files, as well as their cover pages, which are not structured according to specific criteria should not fall within the scope of this Regulation.
>
> Recital 16: This Regulation does not apply to issues of protection of fundamental rights and freedoms or the free flow of personal data related to activities which fall outside the scope of Union law, such as activities concerning national security. This Regulation does not apply to the processing of personal data by the Member States when carrying out activities in relation to the common foreign and security policy of the Union.
>
> Recital 19: The protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and

the prevention of threats to public security and the free movement of such data, is the subject of a specific Union legal act. This Regulation should not, therefore, apply to processing activities for those purposes. However, personal data processed by public authorities under this Regulation should, when used for those purposes, be governed by a more specific Union legal act, namely Directive (EU) 2016/680 of the European Parliament and of the Council. Member States may entrust competent authorities within the meaning of Directive (EU) 2016/680 with tasks which are not necessarily carried out for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and prevention of threats to public security, so that the processing of personal data for those other purposes, in so far as it is within the scope of Union law, falls within the scope of this Regulation.

With regard to the processing of personal data by those competent authorities for purposes falling within scope of this Regulation, Member States should be able to maintain or introduce more specific provisions to adapt the application of the rules of this Regulation. Such provisions may determine more precisely specific requirements for the processing of personal data by those competent authorities for those other purposes, taking into account the constitutional, organisational and administrative structure of the respective Member State, When the processing of personal data by private bodies falls within the scope of this Regulation, this Regulation should provide for the possibility for Member States under specific conditions to restrict by law certain obligations and rights when such a restriction constitutes a necessary and proportionate measure in a democratic society to safeguard specific important interests including public security and the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and prevention of threats to public security. This is relevant for instance in the framework of anti-money laundering or the activities of forensic laboratories.

Recital 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.

Recital 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.

Recital 170: Since the objective of this Regulation, namely to ensure an equivalent level of protection of natural persons and the free flow of personal data throughout the Union, cannot be sufficiently achieved by the Member States and can rather, by reason of the scale or effects of the action, be better achieved at Union level, the Union may adopt measures, in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty on European Union (TEU). In accordance with the principle of proportionality as set out in that Article, this Regulation does not go beyond what is necessary in order to achieve that objective.

The UK GDPR

54. Under section 3 of the European Union (Withdrawal) Act 2018, the UK saved the GDPR in its entirety. This saved version of the GDPR was amended by

Schedule 1 to The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 ("the 2019 regulations").

55. Section 3(10) of the DPA 2018 defines the saved version of the GDPR as the UK GDPR. Section 205(4) of the DPA 2018 explains that the reference in section 3(10) to the GDPR is to the version of it as modified by the 2019 regulations. Section 3 of the European Union (Withdrawal) Act 2018 incorporates direct EU legislation operative immediately before IP completion day (31 December 2020) as part of domestic law on and after IP completion day. The definition of direct EU legislation in section 3(2) includes the GDPR.

56. The saved, and amended, version of the GDPR that became the UK GDPR provides the following Articles relevant to this appeal:

"Article 2

Material scope

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, and

   (b) processing in the course of an activity which, immediately before IP completion day, fell within the scope of Chapter 2 of Title 5 of the Treaty on European Union (common foreign and security policy activities).

1A. This Regulation also applies to the manual unstructured processing of personal data held by an FOI public authority.

2. This Regulation does not apply to-

   (a) the processing of personal data by an individual in the course of a purely personal or household activity;

   (b) the processing of personal data by a competent authority for any of the law enforcement purposes (see Part 3 of the 2018 Act);

   (c) the processing of personal data to which Part 4 of the 2018 Act (intelligence services processing) applies.

…"

"Article 3

Territorial scope

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).
>
> 3. This Regulation applies to the processing of personal data by a controller not established in the United Kingdom, but in a place where domestic law applies by virtue of public international law."

57. For the purposes of this appeal, we are particularly concerned with Article 2(1)(a), Article 3(2)(b) and Article 3(2A). Article 3(2) is in the same terms as Article 3(2) of the GDPR as regards territorial scope. While the route by which processing "in the course of an activity which falls outside the scope of Union law" is excluded from scope differs in the two GDPRs (being via Article 3(2A) in the UK GDPR), the concept is similarly expressed in both Article 2(2)(a) GDPR and Article 2(1)(a) of the UK GDPR. Accordingly, for the purposes of this appeal, there is no material difference between the GDPR and the UK GDPR and we have focused our analysis upon the GDPR provisions.

The 95 Directive

58. Before the GDPR was legislated, processing of personal data in the EU was addressed by Directive 95/46/EC ("the 95 Directive"). The relevant provision of the 95 Directive is Article 3(2). It provides:

> 2. This Directive shall not apply to the processing of personal data:
>
> - in the course of an activity which falls outside the scope of Community law, such as those provided for by Titles V and VI of the Treaty on European Union and in any case to processing operations concerning public security, defence, State security (including the economic well-being of the State when the processing operation relates to State security matters) and the activities of the State in areas of criminal law,
>
> - by a natural person in the course of a purely personal or household activity.

59. The 95 Directive refers to the earlier 1997 Consolidated Version of the Treaty on European Union. Title V was concerned with the responsibilities of the Union and the Member States in respect of a "Common Foreign and Security Policy". Title VI addressed provisions on "Police and Judicial Cooperation in Criminal Matters".

The Law Enforcement Directive

60. As we have set out above, Article 2(2)(d) of the GDPR excludes from scope the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties. Such processing is addressed by a specific

directive applicable to law enforcement: Directive (EU) 2016/679 ("the Law Enforcement Directive").

61. A "competent authority" is defined by Article 3(7) of the Law Enforcement Directive in the following terms:

> "(a) any public authority competent for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security; or
>
> (b) Any other body or entity entrusted by Member State law to exercise public authority and public powers for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security".

State immunity and foreign act of state

62. State immunity is an established rule of customary international law which requires states to accord each other immunity from the jurisdiction of their domestic courts in respect of their sovereign acts: per Lord Sumption JSC in ***Belhaj v Straw*** [2017] UKSC 3, [2017] AC 964 ("***Belhaj***") at [181]. Lord Sumption explained that the rule is derived from the principle of the sovereign equality of states, which is one of the fundamental principles of the international legal order.

63. The UK originally gave effect to this rule of international law by the common law and, more recently, it has been codified in the State Immunity Act 1978: ***Belhaj*** at [182]. Section 14(2) of the Act extends state immunity to "separate entities" (which may be private companies) if the separate entity does anything in the exercise of sovereign authority in circumstances where the state would have been immune had it done the act itself.

64. Section 14 of the State Immunity Act provides:

> **"14 States entitled to immunities and privileges.**
>
> (1) The immunities and privileges conferred by this Part of this Act apply to any foreign or commonwealth State other than the United Kingdom; and references to a State include references to—
>
> (a) the sovereign or other head of that State in his public capacity;
>
> (b) the government of that State; and
>
> (c) any department of that government,
>
> but not to any entity (hereafter referred to as a "separate entity") which is distinct from the executive organs of the government of the State and capable of suing or being sued.

> (2) A separate entity is immune from the jurisdiction of the courts of the United Kingdom if, and only if—
>
> (a) the proceedings relate to anything done by it in the exercise of sovereign authority; and
>
> (b) the circumstances are such that a State (or, in the case of proceedings to which section 10 above applies, a State which is not a party to the Brussels Convention) would have been so immune.
>
> …"

65. Lord Sumption referred to the exceptions which the Act identified for proceedings relating to private, as opposed to sovereign or public acts. He said that the exceptions depended for their application on the nature or subject matter of the action, commenting: "to that extent it may be described as a subject matter immunity". However, he continued, the basic rule was that state immunity was "a personal immunity from the exercise of jurisdiction, which depends upon the identity of the person sued" (at [182]). Lord Sumption went on to confirm at [183] that, as a matter of both international and domestic law, the categorisation of an act as sovereign depends on its character, not its purpose or underlying motive.

66. The domestic courts have recognised that a foreign state is entitled to claim sovereign immunity for its servants or agents, just as it could if it were sued itself.

67. In ***Jones v Ministry of Interior of Saudi Arabia*** [2006] UKHL 26, [2007] 1 AC (***"Jones"***), at [10], Lord Bingham of Cornhill explained that while the State Immunity Act does not provide expressly for a case where a suit is brought against the servant or agent, there was a wealth of authority to show that in such a case, the foreign state was entitled to claim immunity for its servants as it could if sued itself, and its immunity could not be circumvented by suing its servants or agents.

68. At [12] of ***Jones***, Lord Bingham indicated that international law does not require, as a condition of a state's entitlement to claim immunity for the conduct of its servant or agent, that the latter should have been acting in accordance with their instructions or authority; a state may claim immunity for any act for which it is, in international law, responsible, save where an established exception applies. Agreeing, Lord Hoffmann observed at [74] of ***Jones*** that the cases and other materials on state liability make it clear that the state is liable for acts done under colour of public authority, whether or not they are actually authorised or lawful under domestic or international law. He had confirmed at [69] that the concept of "state" in the State Immunity Act must be construed to include any individual representative of the state acting in that capacity. The official acting in that capacity is entitled to the same immunity as the state itself.

69. In ***Koo Golden East Mongolia v Bank of Nova Scotia and others*** [2007] EWCA Civ 1443, [2008] QB 717 (***"Koo"***), the claimant deposited unrefined gold with the central bank of Mongolia under a contract governed by Mongolian law. The agreement required the bank to keep the gold in safe

custody until the date the claimant sold it to the central bank. The central bank exported a portion of the gold. The claimant believed the refined gold was in the possession of a Canadian bullion bank, so issued proceedings in England against the London branch of that bank. It was accepted that the central bank of Mongolia itself would have state immunity. At [40] Sir Anthony Clarke MR identified the key question as being whether the central bank had entered into the contract with the bullion bank in the exercise of sovereign authority. The Court of Appeal held that the bullion bank was an agent of the central bank of Mongolia for the purpose of the principles in ***Twycross v Dreyfus*** (1877) 5 Ch D 605 ("***Twycross***"), where it was held that it was impermissible to obtain relief against the agents of a foreign state. While in ***Twycross***, the defendants might have been commercial agents for the foreign state in a way different to ***Koo***, the fact that their relationship was between principals did not destroy the immunity. The Court of Appeal emphasised that, as confirmed in ***Jones***, the foreign state's immunity (here in the form of the central bank) could not be circumvented by suing its servants or agents (at [47] of ***Koo***).

70. At [199] and [200] of ***Belhaj***, Lord Sumption addressed the foreign act of state doctrine, contrasting it with the rule of state immunity. He distinguished the act of state doctrine as a subject matter immunity, not a personal one. While state immunity and act of state proceed from the same premise (that there is mutual respect for the equality of sovereign states), act of state is entirely created by common law. It requires states to respect the immunity of other states from their domestic jurisdiction. Lord Sumption explained that the foreign act of state doctrine is, at best, permitted by international law, but is not based on it.

71. Lord Sumption discerned two main considerations underlying the doctrine of foreign act of state. The first consideration is commonly called "comity" but which he preferred to call an awareness that the UK courts are an organ of the United Kingdom. Like any other organ of the UK, the courts must respect the sovereignty and autonomy of other states. Lord Sumption observed that this marks the common law's adoption of the same policy underlying the doctrine of state immunity. The second consideration is that the act of state doctrine is influenced by the constitutional separation of powers (which assigns conducting foreign affairs to the executive). Lord Sumption observed that this is why the court does not itself examine the sovereign status of a foreign state or government but treats the Secretary of State's certificate as conclusive (see [225] of ***Belhaj***).

Material scope: the caselaw

72. The Court of Justice of the European Union ("CJEU") has considered the meaning of the phrase "in the course of an activity which falls outside the scope of Union law" in Article 2(2)(a) GDPR and the like phrase ("in the course of an activity which falls outside the scope of Community law") in Article 3(2) of the earlier 95 Directive, on several occasions. We summarise its decisions at this juncture and will return to consider their significance when we explain our construction of Article 2(2)(a) GDPR under 'Analysis' below.

73. In ***B v Latvijas Republikas Saeima*** (Case C-439/19) ("***Latvijas***"), B received penalty points on their driving licence. The Road Safety Directorate of Latvia

("CSDD") entered those penalty points in the national register of vehicles and their drivers. This information was accessible to the public. According to B, it had been disclosed, for re-use purposes, to a number of economic operators.

74. B lodged a constitutional complaint with the Latvian Constitutional Court to examine whether Article 14(2) of the Law on road traffic was consistent with the fundamental right to respect for private life laid down in Article 96 of the Latvian Constitution.

75. In the main proceedings, the Latvian Parliament confirmed that under Article 14(2) of the Law on road traffic, any person may obtain information relating to penalty points imposed on another person, either by enquiring directly at the CSDD or by using services provided by commercial re-users. Furthermore, that provision was justified by the right of access to information, laid down by the Latvian Constitution. The Latvian Parliament explained that, in practice, disclosing the information in the national register requires a person to provide the national identification number (a unique identifier) of the driver in question.

76. The questions referred to the CJEU included whether Article 10 of the GDPR must be interpreted as applying to the processing of personal data relating to penalty points imposed on drivers for road traffic offences, consisting in the public disclosure of data. The CJEU said it should first be determined whether the information constituted personal data, and the disclosure constituted processing that came under the material scope of the GDPR as defined in Article 2. The CJEU decided the information was personal data within the meaning of Article 4(1) and it decided disclosure by the CSDD to third parties constituted processing within the meaning of Article 4(2).

77. The CJEU decided that disclosure of that information fell within the very broad definition in Article 2(1) of the GDPR's material scope and was not excluded from the material scope of the GDPR by Article 2(2)(a) or (d). At [62] of its judgment, the CJEU decided that the exception in Article 2(2)(a) must, like the other exceptions laid down in Article 2(2), be interpreted strictly. It decided that Article 2(2)(a) and (b) of the GDPR represented partly a continuation of the first indent of Article 3(2) of the 95 Directive.

78. The CJEU concluded at [64] that Article 2(2)(a) and (b) of the GDPR therefore could not be interpreted in broader terms than the exception resulting from the first indent of Article 3(2) of the 95 Directive. As we have set out at [58] above, that provision excluded from the Directive's scope, personal data processing taking place in the course "of an activity which falls outside the scope of Community law, such as those provided for by Titles V and VI of the EU Treaty and in any case…processing operations concerning public security, defence, State security."

79. At [65], the CJEU observed that only the processing of personal data in the course of an activity of the State / State authorities expressly listed in Article 3(2) of the 95 Directive or in the course of an activity which could be classified in the same category was excluded from the scope of that directive. The CJEU said at [66] that it followed from this that Article 2(2)(a) of the GDPR, read in the light of recital 16, must be regarded as being designed only to exclude from the scope of that regulation the processing of personal data carried out by State authorities in the scope of an activity intended to

safeguard national security or of an activity that can be classified in the same category, with the result that the mere fact that an activity is one characteristic of the State or of a public authority, is not sufficient for that exception to apply to it automatically.

80. The CJEU decided that, while activities safeguarding national security are intended to protect essential State functions and the fundamental interests of society, activities relating to road safety do not pursue such an objective and cannot be classified in the category of activities having the aim of safeguarding national security, which are envisaged in Article 2(2)(a) of the GDPR ([67] to [68] of the decision). The exception to material scope given in Article 2(2)(a) therefore did not apply to them.

81. In providing its reasoning at [67], the CJEU expressed agreement with the Advocate General's view set out at [57] and [58] of his Opinion that the activities having the aim of safeguarding national security envisaged in Article 2(2)(a) encompass, in particular, those intended to protect essential State functions and the fundamental interests of society. In this part of his Opinion, the Advocate General reasoned that the EU legislature had specified elsewhere (but in the context of data protection) that national security is to be understood as "State security". He also observed that Article 2(2)(a) GDPR should be seen against the background of Article 4(2) TEU, which provides that the EU is to respect Member States' "essential State functions" and in that respect specifies, by way of example, that national security remains the sole responsibility of each Member State. In this context, the Advocate General opined that Article 2(2)(a) of the GDPR does nothing more than reiterate this constitutional requirement of what must be guaranteed for a State to function.

82. At [65] of its decision in ***Latvijas***, the CJEU referred to the earlier CJEU decision in ***Lindqvist*** (C-101/01) [2004] QB 1014 (***"Lindqvist"***). At [43] of ***Lindqvist***, the CJEU emphasised that the activities mentioned by way of example in the first indent of Article 3(2) of the 95 Directive were activities of the state or state authorities and unrelated to the fields of activities of individuals. At [44] of ***Lindqvist***, the CJEU explained that the activities mentioned as examples in the first indent of Article 3(2) of the 95 Directive are intended to define the scope of the exception provided, with the result that the exception in question only applies to the activities which are expressly listed there, or which can be classified in the same category (*ejusdem generis*).

83. In ***Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems (United States of America and others intervening)*** (Case C-311/18) [2021] 1 WLR 751 (**"*Schrems II*"**), the data subject was an Austrian national who had used a social networking site. He lodged a complaint with the Irish Data Protection Commissioner regarding the processing of his personal data under the GDPR. Mr Schrems complained that the personal data he provided to the Irish subsidiary of the group operating the site was transferred to the United States parent company for processing in the United States. At that point, the parent company was legally required to make the personal data available to certain domestic state defence and security authorities. Mr Schrems argued this was incompatible with Articles 7, 8 and 47 of the Charter of Fundamental Rights of the EU and that the USA offered

insufficient protection of the data, contrary to Articles 2, 45 and 46 of the GDPR.

84. Mr Schrems sought to require the Data Protection Commissioner to suspend or prohibit future transfers of his personal data. The Commissioner brought an action to the High Court so that it could refer questions to the CJEU for a ruling. The first question raised by the referring court was whether Article 2(1) and 2(2)(a), (b) and (d) of the GDPR, read in conjunction with Article 4(2) TEU, must be interpreted as meaning the Regulation applied to the transfer of personal data by an economic operator established in a member state to another economic operator established in a third country, in circumstances where, at the time of transfer (or thereafter) the data was liable to be processed by the third country authorities for the purposes of public security, defence and state security.

85. At [102] of his Opinion, the Advocate General expressed the view that Article 2(2) of the GDPR makes clear that it does not apply to, among others, the processing of personal data in the course of an activity which falls outside the scope of EU law or by the competent authorities for the purposes of protecting public security. The Advocate General explained that in his view these provisions reflect the fact that Article 4(2) of TEU recognises competence in matters of the protection of national security is reserved to Member States.

86. The Advocate General considered that the data transfers referred to in Mr Schrems' complaint were not excluded from the scope of the GDPR by Article 2(2)(a) and that they therefore came within the scope of EU law ([103] of his Opinion). He explained at [104] that the question the CJEU was being asked to determine did not concern the applicability of EU law to any subsequent processing by the US authorities for national security purposes of the data transferred to the USA, which would be excluded from the scope *ratione territoriae* of the GDPR. In other words, the Advocate General considered that subsequent processing by the US authorities would be outside GDPR regulation by application of the provisions in Article 3 on territorial scope, rather than outside material scope by virtue of Article 2(2)(a) (in this regard, also see footnote 11 to his Opinion).

87. At [110] of his Opinion, the Advocate General concluded that EU law applied to a transfer of personal data from a member state to a third country where that transfer forms part of a commercial activity, it being immaterial that the transferred data might undergo, on the part of the third country public authorities, processing intended to protect that third country's national security.

88. At [81] of its decision, the CJEU made clear that the rule in Article 4(2) TEU, according to which, within the EU, national security remains the sole responsibility of each member state, concerns Member States of the EU only. The CJEU explained the rule in Article 4(2) was therefore irrelevant in the present case for the purpose of interpreting Article 2(1) and 2(2)(a), (b) and (d) of the GDPR.

89. At [84] the CJEU observed that in considering whether the operation in question was excluded from the scope of the GDPR under Article 2(2), it

should be noted that Article 2 lays down exceptions to the scope of the Regulation "which must be interpreted strictly".

90. At [86] the CJEU confirmed that the possibility that personal data transferred between two economic operators (Facebook Ireland and Facebook Inc) for commercial purposes might undergo, at the time of transfer, or thereafter, processing for the purposes of public security, defence, and state security by the authorities of that third country, could not remove that transfer from the scope of the GDPR.

91. The CJEU drew support from Article 45(2) of the GDPR which expressly requires the EU Commission, when assessing the adequacy of the protection provided by a third country, to take account, among other things, of "relevant legislation, both general and sectoral, including concerning public security, defence, national security and criminal law, and the access of public authorities to personal data, as well as the implementation of such legislation". At [87] of its decision, the CJEU explained this makes patent that no processing by a third country of personal data for the purposes of public security, defence and state security excludes the transfer in issue from the application of GDPR.

92. At [88] of its decision, the CJEU concluded that such a transfer cannot fall outside the scope of the GDPR on the ground that the data in issue is liable to be processed by the authorities of the third country for the purposes of public security, defence, and state security.

93. In ***Österreichische Datenschutzbehörde v WK*** (Case C-33/22) [2024] 4 WLR 42 (***"WK"***), WK complained that his personal data (his name) was published on the Austrian Parliament's website as a result of a committee of inquiry investigating the country's police state-protection agency. At [37] of its decision, the CJEU again confirmed that the exception to processing falling within material scope of the GDPR, provided for in Article 2(2), must be interpreted strictly (per ***Latvijas*** at [62]).

94. At [41], the CJEU agreed with [84] of the Advocate General's Opinion that the exception to the scope of the GDPR provided for in Article 2(2)(a) refers only to categories of activities which, by their nature, fall outside the scope of Union law. It does not refer to categories of persons, depending on whether they are private or public in nature, or, where the controller is a public authority, to the fact that its tasks and duties fall directly and exclusively within the scope of a given public power, unless that power is connected with an activity which, in any event, falls outside the scope of Union law.

95. The CJEU answered the first question referred, in terms that the first sentence of Article 16(2) of TFEU and Article 2(2)(a) of the GDPR must be interpreted as meaning that an activity cannot be regarded as outside the scope of Union law (and therefore outside the scope of GDPR) for the sole reason that it is carried out by a committee of inquiry set up by a Member State's parliament to exercise its power of scrutiny over the executive ([43] of the judgment).

96. The CJEU emphasised the strict interpretation required of Article 2(2)(a) of GDPR and that this was designed solely to exclude from scope personal data processing carried out by state authorities in the course of an activity intended

to safeguard national security or of an activity that can be classified in the same category (at [45]). At [46], the CJEU indicated that activities with the aim of safeguarding national security are those intended to protect essential state functions and the fundamental interests of society. At [47], the CJEU explained such activities remain the sole responsibility of the Member States, in accordance with Article 4(2) of TEU.

97. Applying that approach, at [50], the CJEU explained that while it is for the Member States, in accordance with Article 4(2) of TEU, to define their essential security interests and to take appropriate measures to ensure internal and external security, the mere fact a national measure has been taken for the purpose of protecting national security cannot render EU law inapplicable and exempt the Member States from having to comply with EU law. At [51], the CJEU referred back to its analysis at [41] and emphasised that the fact that a controller is a public authority whose main activity is to ensure national security, cannot be sufficient to exclude that controller's personal data processing from the GDPR when it is in the course of other activities it carries out.

Territorial scope: the caselaw

98. There is one domestic appellate authority that considers the proper interpretation of Article 3(2) of the GDPR. In ***Soriano v Forensic News LLC and others*** [2021] EWCA Civ 1952, [2022] QB 533 (***"Soriano"***), the claimant had joint Israeli and British citizenship and was domiciled in the UK. He brought a defamation claim against five defendants domiciled in the United States of America. The first defendant was a Californian corporation that owned and operated a news publication via a website, Twitter account, Facebook page and podcasts. The second to fifth defendants were journalists who contributed to the first defendant's website. The claim related to online articles and social media posts published by the defendants that referred to Mr Soriano in unflattering terms.

99. The issue before the court was Mr Soriano's application for permission to serve the claim on the defendants outside the jurisdiction, in relation to which an applicant has to show (amongst other criteria) that the claim has a real, as opposed to a fanciful, prospect of success. The judge granted the opposed application in part. On appeal to the Court of Appeal, Mr Soriano cross-appealed against the first instance judge's refusal to allow service of his claims in data protection and malicious falsehood. The former of these challenges required the Court of Appeal to consider issues about the territorial scope of the GDPR.

100. The GDPR applied in the case because Mr Soriano brought his claim before 31 December 2020, when the post-Brexit transition period came to an end and the GDPR ceased to apply directly. Warby LJ, with whom the rest of the Court agreed, explained that the Court of Appeal's decision was not merely of historic interest, because the claim extended to processing after 31 December 2020, some of the continued processing had taken place in the EU and the content of the GDPR had been adopted, with appropriate amendments within UK law, as the UK GDPR (see [73] of the judgment). Mr Soriano brought his claim on the basis that the data processing about which he complained fell within the ambit of Article 3 of the GDPR in terms of territorial scope.

101. At [77] to [78], Warby LJ addressed the meaning of Article 3(1). At [78], he explained that the jurisprudence relating to this part of the Directive was summarised by the European Data Protection Board ("EDPB") in its guidelines (3/2018) on the territorial scope of the GDPR (Article 3) (version 2.1 – revised formatting on 07 January 2020) ("the EDPB Guidelines"), which he indicated are not binding, but relevant.

102. At [82] of ***Soriano***, Warby LJ referred to page 20 of the EDPB Guidelines concerning Article 3(2)(b) (see [119] below) describing this as providing "some assistance". At [100] to [104], Warby LJ analysed Article 3(2). He approached the issue on the basis that Article 3(2)(a) applies to the processing of personal data of data subjects in the Union whether or not they are the same individuals as those to whom the goods or services are offered, providing the two activities are "related to" one another (see [100]). At [101] he concluded that it was arguable that the journalistic processing Mr Soriano complained of was

related to an offer made by the defendants to data subjects in the Union to provide them with services in relation to the form of journalistic output.

103. Turning to Article 3(2)(b), Warby LJ explained that, for similar reasons, it was also arguable that Mr Soriano's case fell within this provision. Warby LJ rejected the argument that publishing articles containing Mr Soriano's personal data was itself a form of "monitoring" within Article 3(2)(b) (so as to bring any processing related to the publication within scope). Warby LJ assessed this as artificial and said it distorted the meaning of the word "monitoring" as used in this context (see [102] of the judgment).

104. Warby LJ identified, however, a more compelling case under Article 3(2)(b), namely that someone who uses the internet to collect information about the behaviour in the EU of an individual who is in the EU, and then assembles, analyses and orders that information for the purposes of writing and publishing an article about that behaviour in (among other places) the EU, would thereby be engaging in "the monitoring of the [data subject's] behaviour….within the Union" within the meaning of Article 3(2)(b). Warby LJ explained that the publication of personal data is clearly a form of "processing", and the preparatory activities are plainly integral to that processing. He decided it follows that the GDPR applies in such a case on the footing that publication amounts to a "processing of personal data of [the data] subject" which is "related to" the monitoring (see [102] of the judgment).

105. Warby LJ assessed this interpretation against Recital (24) to the GDPR and the EDPB Guidelines and concluded it was not fanciful. He observed that the mere fact that the defendants created a collection of personal data relating to Mr Soriano's behaviour in the EU might not be enough to amount to monitoring. However, what they were alleged to have done was to assemble, analyse, sort and reconfigure such data and then publish the results in articles. Warby LJ considered it arguable that those activities fell within the meaning of "monitoring" and therefore within the scope of the EDPB's notions of "behavioural analysis and profiling" (see [103] of ***Soriano***).

106. In ***Google LLC v Commission nationale de l'informatique et des libertes (CNIL) (Wikimedia Foundation Inc and others intervening)*** (Case C-507/17 – [2020] 1 WLR 1993) (***"Google v CNIL"***), the French data protection authority ("CNIL") served notice on Google, requiring that when granting a request to remove links to certain web pages generated by searching the data subject's name (a "de-referencing" request), Google had to apply it to links displayed by all versions of its search engines (not just those in France). Google refused to comply with the notice and only removed links displayed by versions of its search engine whose domain name corresponded to an EU member state, although it also proposed blocking internet users accessing search results from an IP address located in the state of residence of the data subject, no matter which domain name extension they used.

107. CNIL found that Google had failed to comply with its notice and imposed a financial penalty. Google sought annulment of that adjudication and appealed against the financial penalty. The French court stayed the proceedings and referred to the CJEU questions about the territorial scope of de-referencing in light of Articles 12 and 14 of the 95 Directive. Before the CJEU considered the

reference, the 95 Directive was repealed, following which the GDPR applied, Article 17 of which contained the right to de-referencing.

108. As the CJEU indicated at [52], the processing in question was carried out within the framework of Google's establishment in French territory, so the Court proceeded on the basis that the circumstances fell within the territorial scope of the 95 Directive and the GDPR. As regards the latter, see Article 3(1) of the GDPR at [51] above. As we shall return to in our analysis of Clearview's reliance on this case, the CJEU was concerned with the territorial reach of the specific provisions in the 95 Directive and the GDPR addressing de-referencing.

109. The CJEU explained that the objective of the 95 Directive, and the GDPR, was to guarantee a high level of protection of personal data around the EU. At [57] of its judgment, the CJEU expressed the view that in a global world, internet users' access (including non-EU users' access) to links to information about a person whose centre of interests is based in the EU, is likely to have immediate and substantial effects on that person. The CJEU stated that these considerations are sufficient to justify the EU legislature having competence to lay down an obligation to de-reference on all the search engine operator's versions (on request).

110. However, the CJEU observed that numerous third states do not recognise a right to de-referencing or take a different approach to that right (at [59] of the judgment). It also acknowledged that the right to protect personal data is not absolute, but must be considered in relation to its function in society and be balanced against other fundamental rights so that it is proportionate. The CJEU also commented that the balance between the right to privacy and protection of personal data (on the one hand) and freedom of internet users (on the other), is likely to vary significantly around the world (at [60] of the judgment).

111. At [62], the CJEU stated that it was not apparent from the wording of Article 12(b) and 14(a) of the 95 Directive (and Article 17 of the later Regulation) that for the purpose of ensuring the objective of the Directive or, as the case may be, the GDPR, the EU legislature would have chosen to give scope beyond the territory of the Member States to the rights protected by the EU legislation. Nor was it apparent that the EU legislature would have intended to impose a de-referencing obligation on Google and equivalent search engine operators that went beyond the EU Member States.

112. The CJEU also took into account that although the GDPR gives Member State authorities instruments and mechanisms that allow them to co-operate on a cross-border basis within the EU, EU law does not currently provide for these in relation to de-referencing outside the EU.

113. The CJEU therefore decided there was currently no obligation under EU law for a search engine operator who grants a de-referencing request by a data subject, to de-reference on all versions of its search engine (at [64]).

114. At [72] of its judgment, the CJEU emphasised that while EU law does not require de-referencing across all versions of the search engine, neither does it prohibit it. Thus, a supervisory or judicial authority of a Member State

remains competent to weigh up, in light of national standards of protecting fundamental rights, a data subject's right to privacy and personal data protection against the rights of freedom of information. The CJEU observed that it remains open to such an authority, after weighing those rights against each other, to order (where appropriate) the search engine operator to de-reference on all versions of its search engine.

The Travaux in respect of the GDPR

115. In ***Secretary of State for Environment, Food and Rural Affairs v (1) Pickering Fishery Association and (2) Environment Agency*** [2025] EWCA Civ 378 (***"Pickering"***), the Court of Appeal proceeded on the basis that the Travaux prepared by the EU Commission, including a water policy document, were relevant to interpreting the approach envisaged under an EU Directive (see [124] to [127] of the judgment).

116. In 2012, before the Member States legislated the GDPR, the EU Commission identified policy objectives to address. These were to: (a) enhance the internal market dimension of data protection, (b) increase the effectiveness of the fundamental right to data protection and (c) establish a comprehensive EU data protection framework and enhance the coherence and consistency of EU data protection rules. The Commission Staff Working Paper Impact Assessment (Brussels, 25.01.2012, SEC (2012) 72 FINAL), set out a range of policy options to address these policy objectives and associated problems.

117. One problem identified in the Impact Assessment was gaps in current harmonisation causing harmful fragmentation. The Impact Assessment included the following (with the words relied upon by Clearview italicised):

> "b) if the new instrument is a Regulation, the latter would be the law applicable throughout the EU. *The Regulation would also be applicable to 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.*"

118. The EU Commission produced a communication to the European Parliament and the Council in 2016 regarding Transatlantic Data Flows: Restoring Trust through Strong Safeguards (Brussels, 29.02.16 COM (2016) 117 Final). In section 2, the Commission dealt with the EU Data Protection reform. It described the GDPR, and stated the following about territorial scope at section 2.2 (with the words relied upon by Clearview italicised):

> "**2.2 What has changed?**
>
> The Regulation updates, modernises and in some cases strengthens the data protection principles enshrined in the 1995 Data Protection Directive to guarantee privacy rights. It focuses on reinforcing individuals' rights, deepening the EU internal market, ensuring stronger enforcement of the rules, streamlining international transfers of personal data and setting global data protection standards. The rules are designed to make sure that EU individuals' personal data are protected – no matter where they are sent, processed or stored -

even outside the EU, as may often be the case in the digital world. A number of features in the reform are particularly relevant to highlight.

First, **territorial scope**: *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.* Companies based outside the EU will have to apply the same rules as companies based in the EU. This ensures the comprehensive protection of EU individuals' rights. It also creates a level playing field between EU and foreign companies, thereby avoiding competitive imbalances between EU and foreign companies when operating in the EU or targeting consumers in the EU."

The EDPB Guidelines

119. The EDPB Guidelines provide the following guidance that is relevant to territorial scope and the correct interpretation of Article 3(2)(b):

"As a general principle, the EDPB asserts that where the processing of personal data falls within the territorial scope of the GDPR, all provisions of the Regulation apply to such processing. These guidelines will specify the various scenarios that may arise, depending on the type of processing activities, the entity carrying out these processing activities or the location of such entities, and will detail the provisions applicable to each situation. It is therefore essential that controllers and processors, especially those offering goods and services at international level, undertake a careful and *in concreto* assessment of their processing activities, in order to determine whether the related processing of personal data falls under the scope of the GDPR.

The EDPB underlines that the application of Article 3 aims at determining whether a particular processing activity, rather than a person (legal or natural), falls within the scope of the GDPR. [*page 5 of Guidelines*]

…

The application of the "targeting criterion" towards data subjects who are in the Union, as per Article 3(2), can be triggered by processing activities carried out by a controller or processor not established in the Union which relate to two distinct and alternative types of activities provide that these processing activities relate to data subjects that are in the Union. In addition to being applicable only to processing by a controller or processor not established in the Union, the targeting criterion largely focuses on what the "processing activities" are "related to", which is to be considered on a case-by-case basis.

The EDPB stresses that a controller or processor may be subject to the GDPR in relation to some of its activities but not subject to the GDPR in relation to other processing activities. The determining element to the territorial application of the GDPR as per Article 3(2) lies in the consideration of the processing activities in question.

In assessing the conditions for the application of the targeting condition, the EDPB therefore recommends a twofold approach, in order to determine first that the processing relates to personal data of data subjects who are in the Union, and second whether processing relates to the offering of goods or services or to the monitoring of data subjects' behaviour in the Union.

a) Data subjects in the Union

The wording of Article 3(2) refers to "personal data of data subjects who are in the Union". The application of the targeting criterion is therefore not limited by the citizenship, residence or other type of legal status of the data subject whose personal data are being processed. Recital 14 confirms this interpretation and states that *"[t]he protection afforded by this Regulation should apply to natural persons, whatever their nationality or place of residence, in relation to the processing of their personal data*."

This provision of GDPR reflects EU primary law which also lays down a broad scope for protection of personal data, not limited to EU citizens, with Article 8 of the Charter of Fundamental Rights providing that the right to the protection of personal data is not limited but is for "everyone". [*page 14 of Guidelines*]

…

The requirement that the data subject be located in the Union must be assessed at the moment when the relevant trigger activity takes place, i.e. at the moment of offering of goods or services or the moment when the behaviour is being monitored, regardless of the duration of the offer made or monitoring undertaken.

…

The EDPB also wishes to underline that 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, either by offering goods or services to them, or by monitoring their behaviour (as further clarified below), must always be present in addition. [*page 15 of Guidelines*]

…

For Article 3(2)(b) to trigger the application of the GDPR, the behaviour monitored must first relate to a data subject in the Union and, as a cumulative criterion, the monitored behaviour must take place within the territory of the Union.

The nature of the processing activity which can be considered as behavioural monitoring is further specified in Recital 24 which states that *"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." While Recital 24 exclusively relates to the monitoring of a behaviour through the tracking of a person on the internet, the EDPB considers that tracking through other types of network or technology involving personal data processing should also be taken into account in determining whether a processing activity amounts to a behavioural monitoring, for example through wearable and other smart devices. [*page 19 of Guidelines*]

As opposed to the provision of Article 3(2)(a), neither Article 3(2)(b) nor Recital 24 expressly introduce a necessary degree of "intention to target" on the part of the data controller or processor to determine whether the monitoring activity would trigger the application of the GDPR to the processing activities. However, 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. The EDPB does not consider that any online collection or analysis of personal data of individuals in the EU would automatically count as "monitoring", It will be necessary to consider the controller's purpose for processing the data and, in particular, any subsequent behavioural analysis or profiling techniques involving that data. The EDPB takes into account the wording of Recital 24, which indicates that to determine whether processing involves monitoring of a data subject behaviour, the tracking of natural persons on the Internet, including the potential subsequent use of profiling techniques, is a key consideration.

The application of Article 3(2)(b) where a data controller or processor monitors the behaviour of data subjects who are in the Union could therefore encompass a broad range of monitoring activities, including in particular:

- Behavioural advertisement
- Geo-localisation activities in particular for marketing purposes
- Online tracking through the use of cookies or other tracking techniques such as fingerprinting
- Personalised diet and health analytics services online
- CCTV
- Market surveys and other behavioural studies based on individual profiles
- Monitoring or regular reporting on an individual's health status [*page 20 of Guidelines*]

…

Example 18: An app developer established in Canada with no establishment in the Union monitors the behaviour of data subjects in the Union and is therefore subject to the GDPR, as per Article 3(2)(b).

The developer uses a processor established in the US for the app optimisation and maintenance purposes.

In relation to this processing, the Canadian controller has the duty to only use appropriate processors and to ensure that its obligations under the GDPR are reflected in the contract or legal act governing the relation with its processor in the US, pursuant to Article 28.

…

When it comes to a data processor not established in the Union, in order to determine whether its processing may be subject to the GDPR as per Article 3(2), it is necessary to look at whether the processing activities by the processor "are related" to the targeting activities of the controller.

The EDPB considers that where processing activities by a controller relates to the offering of goods or services or to the monitoring of individuals' behaviour in the Union ('targeting'), any processor instructed to carry out that processing activity on behalf of the controller will fall within the scope of the GDPR by virtue of Art 3(2) in respect of that processing.

The 'Targeting' character of a processing activity is linked to its purposes and means; a decision to target individuals in the Union can only be made by an entity acting as a controller. Such interpretation does not rule out the possibility that the processor may actively take part in processing activities related to carrying out the targeting criteria (i.e., the processor offers goods or services or carries out monitoring actions on behalf of, and on instruction from, the controller).

The EDPB therefore considers that the focus should be on the connection between the processing activities carried out by the processor and the targeting activity undertaken by a data controller.

Example 19: A Brazilian company sells food ingredients and local recipes online, making this offer of good available to persons in the Union, by advertising these products and offering the delivery in the France, Spain and Portugal [sic]. In this context, the company instructs a data processor also established in Brazil to develop special offers to customers in France, Spain and Portugal on the basis of their previous orders and to carry out the related data processing.

Processing activities by the processor, under the instruction of the data controller, are related to the offer of good to data subject in the Union. Furthermore, by developing these customised offers, the data processor directly monitors data subjects in the EU. Processing by the processor are [sic] therefore subject to the GDPR, as per Article 3(2).

Example 20: A US company has developed a health and lifestyle app, allowing users to record with the US company their personal indicators (sleep time, weight, blood pressure, heartbeat, etc…). The app then provide users with daily advice on food and sport recommendations. The processing is carried out by the US data

> controller. The app is made available to, and used by, individuals in the Union. For the purpose of data storage, the US company uses a processor established in the US (cloud service provider).
>
> To the extent that the US company is monitoring the behaviour of individuals in the EU, in operating the health and lifestyle app it will be 'targeting' individuals in the EU and its processing of the personal data of individuals in the EU will fall within the scope of the GDPR under Art 3(2).
>
> In carrying out the processing on instructions from, and on behalf of, the US company the cloud provider / processor is carrying out a processing activity 'relating to' the targeting of individuals in the EU by its controller. This processing activity by the processor on behalf of its controller falls within the scope of the GDPR under Art 3(2)." [*page 21 of Guidelines*]

The burden of proof in appeals against ICO Notices

120. In ***Doorstep Dispensaree Ltd v Information Commissioner*** [2024] EWCA Civ 1515 (***"Doorstep Dispensaree"***), the Court of Appeal addressed where the burden of proof lies when someone on whom the ICO has imposed a penalty under section 155 of the DPA 2018, appeals against it. Counsel for Doorstep Dispensaree argued that while the DPA 2018 does not expressly provide for the ICO to bear the burden of proof on an appeal under section 163 of the Act, this was implicit. He argued that where the imposition of a penalty is in issue, it is for the body imposing that penalty to justify it (see [38] of ***Doorstep Dispensaree***).

121. Newey LJ, with whom the rest of the Court of Appeal agreed, rejected this proposition and held that the burden of proof lies on the appellant in an appeal against the imposition of a penalty under section 155 of the DPA 2018. He acknowledged that before raising a penalty notice, the ICO must be satisfied that one of the conditions in section 155(1)(a) and (b) of the DPA 2018 is met and that it is appropriate to require the person to pay the penalty. Newey LJ decided, however, that where the recipient of a penalty notice appealed under section 163, it was incumbent on him to persuade the FTT that the penalty should not stand.

122. At [39], Newey LJ placed reliance on the general principle enunciated by Carnwath LJ in ***Khan v HM Revenue and Customs*** [2006] EWCA Civ 89 (***"Khan"***), that "…where a state gives a right of appeal against enforcement action taken by a public authority, the burden of establishing the grounds of appeal lies on the person appealing" and the "ordinary presumption…is that it is for the appellant to prove his case" (see [71] and [73] of ***Khan***). Newey LJ indicated that far from suggesting that this general principle was limited to the refusal of benefits rather than the imposition of penalties, Carnwath LJ had explained that it applied to enforcement notices in respect of breaches of planning control and that this approach represented the correct starting point in relation to an appeal against a civil penalty.

123. Newey LJ noted at [39] that in ***Doorstep Dispensaree***, as in ***Khan***, the appellant, rather than the ICO, knew or was in a position to know, the true

facts. Newey LJ also confirmed that the fact that the FTT considers matters "afresh" on an appeal under section 163 of the DPA 2018 was not inconsistent with the appellant bearing the burden of proof. He concluded that the burden of proof on an appeal against a penalty notice lay throughout on the appellant (see [40] and [41] of the judgment).

124. Having concluded that in a full merits review the FTT will normally be able to decide whether a penalty is justified without resorting to the burden of proof, Newey LJ confirmed that where that is not the case, the burden is on the appellant, not the ICO (see [42] of the judgment).

Analysis

Article 2(2)(a) GDPR: material scope

125. The first major issue we had to consider was whether any of the four exclusions in Article 2(2) GDPR applies to take Clearview's processing outside the material scope of regulation under the GDPR and, given the way that Article 2(1) of the UK GDPR operates, outside the UK GDPR. Of the four exclusions in Article 2(2), it was agreed that only two were relevant to the circumstances of this appeal:

    a. Article 2(2)(a), which excludes processing "in the course of an activity which falls outside the scope of Union law"; and

    b. Article 2(2)(d), which excludes processing "by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security".

The parties' positions on material scope in brief

126. The meaning of the phrase "in the course of an activity which falls outside the scope of Union law" lies at the heart of this appeal.

127. While the parties agreed that the ICO has no jurisdiction to take enforcement action against foreign states in respect of their data processing in the context of their national security or law enforcement functions, they disagreed as to the mechanism for that restriction.

128. Mr Pitt-Payne KC, for the ICO, argued that any proper interpretation of Article 2(2)(a) of the GDPR must be informed by the principles of public international law that govern the relationships between states. These principles were referred to by the parties variously in terms of "international comity", "sovereign equality of states", "state immunity", and "act of state doctrine". We use "comity principles" as an umbrella term to cover these principles. Mr Pitt-Payne maintained that, viewed through the lens of comity principles, the words "in the course of an activity which falls outside the scope of Union law" in Article 2(2)(a) refer to all matters that are without the competence of the Union: not only matters reserved to Member States, but also activities of foreign states with which neither the Union nor its Member States presume to interfere for reasons of comity.

129. Ms Demetriou KC, for Privacy International, argued for a much narrower interpretation: Article 2(2)(a) was concerned, she said, only with the division of responsibilities as between the Union and its Member States. It had no need to say anything about the activities of foreign states, because the GDPR is not concerned with the activities of foreign states at all. On Privacy International's construction, the words "an activity which falls outside the scope of Union law" refer only to those activities in respect of which Member States have reserved control to themselves and conferred no powers on the Union to act. Examples of such activities are matters of national security, foreign policy and certain species of taxation.

130. Mr Pitt-Payne and Ms Demetriou both agreed, however, that their respective interpretations amounted to "different paths up the same mountain", and whichever of their interpretations was correct, the outcome would be the same: data processing carried out by foreign states was beyond the ICO's jurisdiction. Although they did not share the same analysis, they agreed that the issue whether Clearview or its private sector contractor clients were also excluded from regulation depended on the application of comity principles. The ICO's analysis was that any exclusion would be under Article 2(2)(a). Ms Demetriou argued it would instead be on a freestanding basis.

131. Ms Proops KC, for Clearview, proposed a different explanation of what Article 2(2)(a) addresses, and how it should be interpreted. Ms Proops argued that the provision's focus was neither on the activities of foreign states (which the Union was prevented from regulating both as a matter of competence and as a matter of public international law), nor on the national security activities of Member States (as these were reserved to the national governments of Member States by the terms of the TEU). Ms Proops invoked the principle that lawmakers do not legislate in vain. She said the EU legislators must have intended to achieve something more than simply confirming that the Regulation did not extend to activities that were already excluded from regulation.

132. Ms Proops said the key to unlocking what Article 2(2)(a) was about, was understanding the policy intent behind it. This policy intent was to avoid "a kind of back door regulation" of foreign states by regulating third parties whose processing occurs "in the course of" activities that are quintessentially state functions, such as matters of national security or law enforcement. She argued that such back door regulation would amount to "the most serious type of comity offence".

133. Ms Proops submitted that, taking a purposive construction, Article 2(2)(a) must apply to remove Clearview's processing from the material scope of the GDPR. This was because, at the point at which a client uploads a 'probe image' to initiate a search of Clearview's databases for potentially matching vectors, Clearview's processing "intersects so fundamentally" with its client's processing that Clearview's processing and its client's discharge of its state functions are "effectively merged" such that they cannot be disentangled. Thus, Clearview's processing is (in the words of Article 2(2)(a)) carried out "in the course of an activity which falls outside the scope of Union law". Ms Proops referred to this as her "intersectional construction", and we shall refer to it in the same terms.

What the FTT decided in relation to Article 2(2)(a)

134. Because we are tasked with deciding whether the FTT erred materially in law in deciding that Clearview and its private sector contractor clients fell outside the material scope of regulation under Article 2(2)(a), it is necessary for us to seek to understand how the FTT interpreted and applied Article 2(2)(a) GDPR. We have set out the FTT's reasoning in full at [17] above.

135. Unfortunately, the reasons the FTT gave for its decision-making on material scope are very sparse indeed. The ICO and Clearview interpret them very differently.

136. Mr Pitt-Payne submitted that the FTT's decision that Clearview's own processing was excluded from material scope under Article 2(2)(a) proceeded on one of two possible bases:

    a. Clearview was itself discharging foreign state functions when it provided its Service to its clients; or

    b. Clearview fell to be equated with, or effectively merged with, or treated as standing in the shoes of, its clients for the purposes of the application of Article 2(2)(a).

137. Mr Pitt-Payne maintained there was no basis in law for either.

138. Ms Proops accepted that, had the FTT reached its decision on either of the bases suggested by Mr Pitt-Payne, it would have erred in law. However, she says it is tolerably clear from the FTT's decision, when read as a whole, that it fell into no such error.

139. Rather, having made an unequivocal finding based on unchallenged evidence (expressed at [26(a)] and [146] of the FTT's decision) that all of Clearview's clients "carry out criminal law enforcement and/or national security functions, and use the Service in furtherance of those functions", the FTT decided that Clearview's own processing in delivering the Service intersected sufficiently with its clients' state functions that it could properly be concluded that Clearview's processing was done "in the course of" its clients' out of scope state functions and was therefore excluded from material scope under Article 2(2)(a).

140. Ms Proops argued, in other words, that the FTT adopted precisely the intersectional construction that she commended to us at the Upper Tribunal hearing.

141. At [154] of its decision, the FTT states that it has concluded that Clearview's processing activities are outside material scope by virtue of Article 2(2)(a). It says it has done so "for all these reasons". This encouraging phrase suggests that the conclusion must be preceded, or possibly followed, by an articulation of at least the principal reasons for that conclusion. However, a thorough search of the 153 paragraphs that precede it, and the five that follow it, reveals scant reasoning on this central issue in the appeal, including an absence of any analysis of the meaning of the wording of Article 2(2)(a) ("in the course of an activity which falls outside the scope of Union law") or any reference to the caselaw of the CJEU where this has been considered.

142. At the hearing we invited Ms Proops to identify the reasons to which [154] refers. She took us to the finding in [146] to which we have already referred in [139] above. She pointed out that in [146] of its decision, the FTT rejected the ICO's suggestion that Clearview's clients used the Service for purposes other than the discharge of state functions. She said this was "another reason" that the FTT relied on in coming to its conclusion. She pointed further to the FTT's rejection of the ICO's argument that Clearview might offer the Service to

commercial clients in future, which the FTT said was irrelevant to the application of Article 2(2)(a) (see [147] to [148] of the FTT's decision). Ms Proops said the conclusion in [154] that Clearview's processing "was in the course of an activity which … fell outside the scope of EU law" was grounded in this "cumulative reasoning".

143. Ms Proops submitted further that the FTT's conclusion could not have been reached on either of the bases suggested by Mr Pitt-Payne because its decision contained no reasoning to that effect. Ms Proops commented that this was unsurprising, both because no such argument had been put to the FTT, and because any such argument would have been wholly misconceived.

144. We are unpersuaded that there is any "cumulative reasoning" to support the FTT's conclusion as to the applicability of Article 2(2)(a) to Clearview. Its rejection of the ICO's claim that Clearview's clients use the Service for purposes other than discharging their criminal law enforcement and/or national security functions does not amount to a reason for its conclusion: it is just another way of expressing the finding it had already made that Clearview's clients use the Service "exclusively in furtherance of" state functions. There is no accumulation of reasoning. Neither does the FTT's rejection of the ICO's speculative submission about the possibility of Clearview offering the Service to commercial clients in the future add to the reasons. It merely clarifies one aspect that the FTT did not consider it should take into account.

145. So, we are left only with the finding that Clearview's clients use the Service "exclusively in furtherance of" their criminal law enforcement and/or national security functions. That finding, which is itself unexplained, provides a potential foundation for the FTT's conclusion that the processing of personal data by Clearview's clients was "in the course of an activity which … fell outside the scope of Union law", but it does not explain how or why it concluded that Clearview's own processing was not caught. In the absence of such an explanation, the "conclusion" in [154] of the FTT's decision is a *non sequitur.*

146. Ms Proops argued that application of the intersectional construction should be inferred because the FTT provided no analysis on the lines of either of Mr Pitt-Payne's proposed rationalisations for its conclusion in [154]. However, the same observation can be made of the FTT's decision regarding the construction suggested by Ms Proops: the decision provides no analysis that even hints that it might have adopted an intersectional construction either. Ms Proops conceded that the case she put to us on intersectional construction was not the case that Clearview argued before the FTT. Indeed, she conceded that Clearview's case on jurisdiction before the FTT was firmly based on Clearview falling outside *territorial scope* under Article 3(2)(b), rather than it being excluded from *material scope* under Article 2(2)(a). This further weakens the case for inferring that the FTT applied an intersectional construction in reaching its decision and we reject this suggestion.

147. In summary, the FTT set out its conclusion on the application of Article 2(2)(a) but did not provide reasons that are adequate to explain how or why it reached that key conclusion. That failure itself amounts to an error of law, albeit not one that the ICO pursued as a standalone ground.

148. So, where does that leave us in terms of the ICO's appeal Grounds 1 and 2? To decide whether the FTT's error of law was material, we must construe Article 2(2)(a) for ourselves and decide whether the FTT's conclusion accords with our construction.

149. The ICO's Grounds 3 and 4 and Clearview's Additional Reasons 1, 2, 3 and 4 concern the provisions on territorial scope, which was the focus of the proceedings before the FTT. The FTT gave a detailed explanation of its interpretation and application of Article 3(2)(b) of the GDPRs at [115] to [144] of its decision. The ICO's Grounds 3 and 4 and Clearview's Additional Reasons 1 to 4 require us to construe Article 3(2)(b) GDPR and UK GDPR and to decide whether the FTT erred in its interpretation or application in a way that was material.

150. We now turn to the law on the approach that we must take to construing the GDPRs before explaining how we construe those provisions.

General approach to construction of the GDPRs

151. Ms Proops emphasised the broad and weighty nature of the data protection scheme under the GDPRs, highlighting the potentially serious consequences of a breach of their provisions, including mass data protection claims in the civil courts, criminal sanctions for non-compliance (see sections 144, 148 and 173 of the DPA 2018), and the imposition by regulators of large fines and orders to stop processing data. These sanctions could cause significant disruption to a controller's business and might, ultimately, prevent it from operating at all. Ms Proops submitted that the "significant, particularly weighty nature" of the data protection scheme should be a factor that is taken into account when deciding how broadly or narrowly the provisions in issue in this appeal should be construed and applied.

152. Against that backdrop, Ms Proops argued, construction of the GDPR engages four principles of statutory interpretation:

    a. comity;
    b. utility;
    c. legal certainty; and
    d. proportionality.

153. We agree that these principles are relevant, and we have borne them in mind in interpreting these provisions. Counsel for the parties took us to various domestic and EU law authorities to assist us in our task of construction.

Domestic authorities on comity, extra-territoriality and utility

154. Ms Proops drew the panel's attention to several domestic authorities that concerned the proper approach to considering whether, and if so to what extent, domestic statutory provisions are to be construed as having extra-territorial effect.

155. ***R (Al-Skeini and others) v Secretary of State for Defence*** [2007] UKHL 26, [2008] 1 AC 153 (***"Al-Skeini"***) was a House of Lords decision that concerned the territorial application of the Human Rights Act 1998 ("HRA"). The claimants were relatives of Iraqi civilians who had been killed by British soldiers in Iraq.

Relying on Articles 2 and 3 of the European Convention on Human Rights ("ECHR") in conjunction with the HRA, they sought judicial review of the Secretary of State's failure to conduct inquiries into, or to accept liability for, the deaths. Their Lordships held that the HRA did not apply extra-territorially to the circumstances of the deaths in Iraq except in respect of the deaths at UK military bases. This was because, except in relation to its military bases, the UK exercised insufficient control over the relevant territory in Iraq. Lord Bingham (at [11] of his speech) referred to a long line of authority for the principle that, unless the contrary intention appears, "Parliament is taken to intend an Act to extend to each territory of the United Kingdom, but not to any territory outside the United Kingdom" (citing *Bennion, Statutory Interpretation*, 4th ed (2002) at p. 282), and "an enactment applies to all persons and matters within the territory to which it extends, but not to any other persons and matters" (quoting *Bennion* again, at p.306). Lord Bingham said the existence of such a presumption was not in doubt, and he commented that it appeared to have become stronger over the years.

156. Ms Proops suggested the reason for the presumption becoming stronger over time was that the more interconnected the world becomes, the more we look to involve ourselves in the territories and affairs of foreign states, and the more we involve ourselves in the territories and affairs of foreign states, the more important it becomes to ensure robust protection for comity principles.

157. Ms Proops derived two important policy principles from Lord Rodger's speech in ***Al-Skeini*** (at [44] to [45]):

    a. the principle that legislation is to be interpreted "so far as its language permits, so as not to be inconsistent with the comity of nations or the established rules of international law" (invoking *Maxwell on the Interpretation of Statutes,* 12th ed (1969) at p.183); and

    b. the principle of practical utility in cases involving overseas persons who have no presence in the jurisdiction: it 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 UK. So, in the absence of any indication to the contrary, a court will interpret legislation as not intended to affect such people.

158. Ms Proops also relied on the Supreme Court's decision in ***R (KBR Inc) v Director of the Serious Fraud Office*** [2021] UKSC 2, [2022] AC 519 (***"KBR"***), a judicial review brought by KBR, which was the US parent company of UK subsidiaries. The Serious Fraud Office issued a notice to KBR, which had no corporate presence in the UK, under section 2(3) of the Criminal Justice Act 1987 ("CJA") requiring it to produce documents held outside the UK to assist its conduct of a major fraud investigation. KBR maintained that section 2(3) of the CJA did not apply to foreign companies with no presence in the jurisdiction. The Supreme Court agreed on the grounds that section 2(3) contained no express wording to rebut the presumption against extra-territorial effect, and neither was there any clear indication either for or against extra-territorial effect in any other provisions of the CJA. In his judgment (at [28]) Lord Lloyd-Jones discussed the

presumption against extra-territorial effect, and arrived at the following formulation:

> "The 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."

159. Ms Proops argued that, because Lord Lloyd-Jones's statement quoted above followed immediately after his reference to the Bribery Act 2010 ("Bribery Act"), which provides for extra-territorial effect, it followed that his formulation applied not only to the issue whether there was any extra-territorial effect, but also to the extent of the territorial effect of statutory provisions that do provide for extra-territorial effect.

160. We do not agree with Ms Proops' reading of what Lord Lloyd-Jones said. On our reading, section 12 of the Bribery Act was cited as an example of a statute that involved considerable "exorbitance" (the criminalisation of acts done outside the jurisdiction, provided that those acts would be criminal if done in the UK and provided that the actor satisfied one of the criteria for close connection with the UK). Lord Lloyd-Jones was saying nothing more than 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.

161. Ms Proops submitted that what emerges from these authorities is the critical importance, when construing a particular provision of legislation, of identifying very precisely what the purpose of that provision is: what particular objective it was intended to further, and what particular "mischief" it was intended to address.

162. With the exception of our disagreement about what can be taken from Lord Lloyd-Jones's judgment, we do not take issue with any of the general principles outlined above. However, we do not find these domestic authorities to be particularly helpful to Clearview's case on the construction of the GDPR for two reasons:

    a. first, they are domestic authorities that speak to the approach the domestic courts take to construing domestic legislation. Ms Proops said they were nonetheless of assistance because they concern foundational principles that must, as a matter of common sense, apply equally to construing EU legislation as to domestic legislation. However, this sits uneasily with another submission she made to us orally to the effect that it was important to understand that EU law is "a very particular type of law, one that is distinct from the sorts of laws which sovereign legislatures enact", which undermines her reliance on domestic authorities; and

    b. second, and much more importantly, they do not assist Clearview's case because the GDPR and the UK GDPR are expressly stated to have extra-territorial effect (including in each limb of Article 3(2)), and it is abundantly clear from the recitals to the GDPR that the legislators were alive to the implications of providing for extra-territorial effect and

they calibrated the regulatory scheme accordingly (see, in particular, Recitals 23 and 24 GDPR).

EU authorities on extra-territorial effect and comity

163. Ms Proops described the EU as "fundamentally a territorially preoccupied legal edifice" and said this position was reflected in EU caselaw.

164. In ***Air Transport Association of America and others v Secretary of State for Energy and Climate Change*** C-366/10 (***"Air Transport Association of America"***) the CJEU considered a challenge to the EU's emissions trading scheme on the basis that the directive implementing it was in breach of applicable international laws. The CJEU took a territorially confined approach, concluding that the scheme applied only where an aircraft was within an aerodrome within the territory of a Member State, and did not apply to aircraft flying over the high seas, or even flying over the territory of a Member State but not landing there. This was, Ms Proops said, notwithstanding that EU citizens would clearly be better off were the EU to control emissions globally, rather than simply within the territories of the EU.

165. Ms Proops pointed to ***Google v CNIL*** (discussed at [106] to [114] above) as another example of the CJEU taking a territorially confined approach to construction of EU legislation, this time in a data protection context. ***Google v CNIL*** did not involve the application of international law, but it did engage comity considerations, including the imperative to avoid regulating how non-EU actors go about exercising their right to access information online.

166. As we explained in our earlier summary, in ***Google v CNIL*** the CJEU decided that Google's response was compliant even though Google had "geo-fenced" its de-referencing activities with the result that links concerning the requester were de-referenced only in respect of searches conducted from within the EU, and not in respect of searches conducted from outside the EU. This was because the de-referencing provisions in question were essentially territorial in nature, and so applied only within the territories of the EU, even though that meant that EU data subjects' "right to be forgotten" was therefore only partial. Ms Proops said this underlined that data protection rights are fundamentally territorial in nature.

167. We accept this to be an example of a territorially focused approach being taken by the CJEU. However, it represented the CJEU following the wording of the material provisions of the 95 Directive and the GDPR, rather than giving them an artificially narrow interpretation. The EU legislators chose to enact provisions (Articles 12(b) and 14(a) of the 95 Directive, replaced by Article 17 of the GDPR) that prescribed a territorially focused approach. This case is not authority for the proposition that EU legislation must be construed territorially where the provisions themselves do not indicate an intention to be territorially confined.

168. Ms Proops pointed to the objective of the GDPR as explained in Recital 170 as being to ensure an equivalent level of protection "throughout the Union", and not "throughout the world". She said this reflects the principle that EU law generally strives to regulate what happens within, not beyond, the borders of the EU, even when that might result in sub-optimal protection for EU citizens.

169. However, as Ms Proops had to concede, it cannot be said that there could never be any element of extra-territoriality to EU laws to protect the interests of EU citizens. Rather, she said that if provisions are to have extra-territorial effect that effect must be provided for in sufficiently clear terms, and the situation is starker still in relation to the activities of foreign states because the EU simply has no competence to legislate for what foreign states do, or do not do.

170. We agree with Ms Proops that the EU is generally focused on matters within its borders, but we are not persuaded that the authorities she seeks support from really advance Clearview's case. This is for the simple reason that Recitals 23 and 24 GDPR make clear that the legislators had identified a need to regulate extra-territorially in order to protect the data rights of EU data subjects in the digital age, and they introduced express wording into Article 3 to provide for precisely that.

171. Ms Proops made the point that the EU is not a sovereign state in joint dominion over the territories comprised within it, but rather a legal construct through which a collection of sovereign states agree to come together and agree to be bound by a set of common rules on various matters by way of the treaties to which the members signed up, and the legislation made under those treaties. She likened the EU's laws to the rules of a members' club whose rules bind its members because those members have agreed to be bound by them. Ms Demetriou also invoked the analogy between EU legislation and the rules of a members' club. Like them, we find this analogy to be helpful.

172. As a "members' club", the EU's competence extends only to its Member States, and, even then, it extends only to those matters in respect of which its Member States have conferred authority on it to decide. Ms Proops submitted that any construction of EU legislation to the contrary is "legal heresy" and fails to understand the essentially constitutional nature of the EU. She added that, even were the EU to have competence to legislate to control or regulate the acts of foreign states, it is inconceivable that it would exercise that competence so as to create rules that risk capturing the activities of foreign states, whether through the "front door" or the "back door", because to do so would profoundly infringe the principles of comity and sovereign equality. She said that to seek to regulate private actors in the sovereign territories of other nation states raised significant comity and futility issues, but to seek to regulate or control how foreign states function is a "completely different order of comity offence".

173. We find Ms Proops' submissions on the "heresy" of any interpretation that fails to reflect the limits to the EU's competence somewhat puzzling. This is because neither the ICO nor Privacy International has proposed such a construction. Ms Demetriou said Article 2(2)(a) amounts simply to a confirmation that the GDPR does not seek to regulate in respect of matters that had been reserved to the national governments of its Member States, and it says nothing of the position of foreign states. That is very much "on all fours" with what the Advocate General said in his opinion in ***Latvijas*** at [58], namely that Article 2(2)(a) reiterates the constitutional requirement of what must be guaranteed for a State to function: see [81] above.

174. Privacy International's case is not that foreign states are within the material scope of regulation, but rather that they are outside the scope of the GDPR entirely by operation of public international law. That interpretation is unarguably respectful of comity.

175. The ICO's construction of Article 2(2)(a) is that, while it is mainly about the things that Privacy International says it is about, because it must be viewed through the lens of comity principles, the words "outside the scope of Union law" must be read to exclude the activities of foreign states too. That interpretation is likewise perfectly respectful of comity.

Certainty and foreseeability

176. Ms Proops drew our attention to ***Fintan Duff and Others v Minister for Agriculture and Food, Ireland and the Attorney General*** (Case C-63/93) [1996] ECR I-569 as authority for the proposition that EU law requires EU enactments to be clear and precise to ensure that situations and legal relationships governed by EU law are foreseeable (see [18] to [20] of that decision). Ms Proops submitted that the GDPRs had to be construed in a way that rendered them certain and foreseeable. We do not consider this to be a controversial proposition, and we have construed the provisions of the GDPRs in accordance with this principle.

Proportionality

177. Ms Proops also invoked the principle of proportionality, which she said provided another important control on the construction and application of EU laws. She said this principle must inform our construction of the provisions of the GDPR because it would be wholly disproportionate if Clearview were to be made subject to the "legislative behemoth" of the GDPR merely because of *de minimis* activity.

178. As Mr Susskind argued, Article 3(2)(b) of the GDPR does not provide expressly for a *de minimis* principle to be applied. Ms Proops did not provide any authority to support her argument that it should be inferred when Article 3(2)(b) is applied. While we accept that proportionality is an important principle in EU law, and we accept that proportionality would be a relevant consideration when considering the substantive appeal against the Notices, we are not persuaded that proportionality is a relevant consideration in the context of the preliminary issue of whether the ICO had jurisdiction to issue the Notices.

EU law authorities on the construction of Article 2(2)(a) of the GDPR

179. In support of her narrow construction of Article 2(2)(a) Ms Demetriou referred us to a series of decisions of the CJEU that concerned the proper interpretation of the GDPR, and of Article 2(2) in particular.

180. In ***Schrems II*** (summarised at [83] to [92] above), a case decided before the UK's exit from the EU and therefore binding on us, the CJEU held at [84] that, by analogy with Article 3(2) of the 95 Directive, the exceptions provided for in Article 2(2) must be read strictly. This point was developed in the later case of ***Latvijas*** (summarised at [73] to [82] above), which was decided following the

UK's exit from the EU and is therefore of persuasive, rather than binding, authority) the CJEU stated (at [64] to [65]) that Article 2(2(a) of the GDPR could not be interpreted in broader terms than the exception resulting from the first indent to Article 3(2) of the 95 Directive (which had itself been narrowly interpreted in ***Lindqvist***, as we explained at [82] above.

181. The issue before the CJEU in ***Latvijas*** (summarised at [76] to [77] above) was whether the exclusion of "outside scope" activities under Article 2(2)(a) applied only to Member States' national security and similar functions, or whether it should be interpreted more broadly to apply to other Member State functions, such as those relating to road safety, which was the function relevant in that case.

182. The CJEU was not tasked with deciding whether Article 2(2)(a) also applies to foreign state activities, but it is clear from the Advocate General's opinion (at [58]) that he considered Article 2(2)(a) to be nothing more than a restatement of the EU's respect for the reservation by Member States of powers in respect of their essential functions. As we noted earlier, this paragraph of the Attorney General's opinion was endorsed by the CJEU at [67] of its judgment (albeit in the course of highlighting a different point).

183. Ms Proops argued that the CJEU's construction of Article 2(2)(a) was applied in the context only of the specific question of which Member State functions were within scope, and which were outside it, and a narrow reading of the exception was not required in other contexts. She said that the exception created by Article 3(2) of the 95 Directive was drafted deliberately broadly (as she says Article 2(2)(a) GDPR was), with mere examples being given ("such as those provided for by Titles V and Title VI of the Treaty on European Union"), and she did not accept that it was only concerned with the activities of Member States.

184. However, the proposition that Article 3(2) of the 95 Directive was intended to have a broad effect is inconsistent with the CJEU's analysis in ***Lindqvist*** (discussed at [82] above) and in ***Schrems II*** at [89] above, which is binding on us. In further support of Ms Demetriou's reading, we note that the examples given in Article 3(2) of the 95 Directive concern the division of responsibility between the Union and its Member States, and Recital 16 to the GDPR, which concerns the exclusion of "activities which fall outside the scope of Union law", explains that the regulation does not apply to processing "by Member States when carrying out activities in relation to the common foreign and security policy of the Union". This supports Ms Demetriou's case that Article 2(2) of the GDPR only deals with the division of responsibility between the Union and its Member States.

Relevant comity principles

185. We have addressed the nature and scope of state immunity at [62] to [71] above, where we have also explained that the foreign act of state doctrine is not based on international law principles.

Our construction of Article 2(2)(a)

186. Applying the principles discussed above, the binding authorities of ***Lindqvist*** and ***Schrems II***, and the persuasive authorities of ***Latvijas*** and ***WK*** (summarised at [95] to [96] above), we conclude that the phrase "an activity which falls outside the scope of Union law" in Article 2(2)(a) GDPR must be construed strictly. The exception created by this wording cannot be interpreted to apply more broadly than the exception given in the 95 Directive.

187. There is nothing in ***Latvijas*** (or indeed in any of the other authorities to which our attention was drawn) to indicate that the CJEU intended to suggest that the requirement for a strict construction of the exception in Article 2(2)(a) was limited to identifying the division of activities between the Union and Member States, as Ms Proops suggested. Rather, we consider the issue whether the exception created by Article 2(2)(a) is to be given a narrow or a wide meaning to be binary - either the exception is to be construed narrowly, or it is not. On that basis, we consider that the CJEU's decision that the exception bears a narrow construction is applicable in all circumstances.

188. Ms Proops pointed out that there was no authority before us concerning the interpretation of Article 2(2)(a) specifically in the context of foreign state activities. She suggested the reason there were authorities about which Member State activities fell within scope of Union law, and which fell outside it (and so within the exception in 2(2)(a)), was because the "carve up" of powers between the EU and Member States was a "tricky matter". Ms Proops suggested the reason there were no authorities about foreign state activities was because it was obvious that <u>all</u> foreign state activities fall outside the scope of Union law, so it did not provide fertile ground for litigation. We do not consider that the absence of any such cases permits an inference that Privacy International's interpretation is likely to be wrong. It just means that the issue has not come before the CJEU.

189. We acknowledge that there is no authority that is directly determinative of the issue of the proper reading of Article 2(2)(a). We accept that the fact that the authorities dealing with its interpretation concern the division of responsibilities between the Union and its Member States does not necessarily preclude it applying in other circumstances. However, neither is there any authority supporting either Mr Pitt-Payne's or Ms Proops' interpretations. We have already noted that in the Advocate General's opinion in ***Schrems II,*** where he observed (at [104]) that subsequent processing by the US State would be excluded from the GDPR, he referred to Article 3, and not to Article 2(2)(a). This suggests that he did not read the exception in Article 2(2)(a) as referring, and applying, to foreign states (see [86] above).

190. We are persuaded that Privacy International's interpretation is to be preferred. That reading is consistent with the characterisation that Ms Proops herself favoured of the EU as a members' club, whose legislation establishes the rules by which its members have agreed to act. Seen through that prism, it would be strange were the club rules to include a provision that deals with the situation of non-members, who have not signed up to the club rules, and who are not bound by them.

191. We accept Ms Demetriou's submission that by the time the GDPR was enacted, the phrase "outside the scope of Union law" already had a recognised meaning in EU legislation. That meaning was not the literal meaning for which Ms Proops advocated (i.e. anything beyond the legislative competence of the Union, howsoever excluded). Rather, it referred to matters reserved to national governments of Member States.

192. We have considered the principle that Parliament does not legislate in vain. Privacy International's construction does not offend against that principle: Article 2(2)(a) serves to confirm, for the reassurance of Member States, that the ambit of the regulation respects the established division of responsibility between the Union and its Member States. That is a legitimate purpose, albeit a modest one, and we note that declaratory provisions with no operative element are by no means unknown in EU legislation.

193. Neither does this construction offend against comity principles in any way, because on this reading, the EU does not presume to interfere with the activities of foreign states at all.

194. By contrast, Clearview's rejection of Privacy International's construction proceeds from the dissonant starting point that the words "processing in the course of an activity which falls *outside* the scope of Union law" (our emphasis added) can *only* refer to processing that is *within* the scope of Union law, and any other interpretation must be rejected. While this logic may appeal to devotees of structural linguistics, it is not by any means an obvious reading and it does not sit well with the principles of certainty and foreseeability that Ms Proops enjoined us to follow when construing these provisions. We consider Privacy International's submitted construction to be a far more natural interpretation of the words of the provision, and the one most consistent with what is said in the GDPR's Recitals (particularly Recital 16).

195. It follows from all of this that we do not accept that the processing activities of Clearview or its clients are excluded by operation of Article 2(2)(a) of the GDPR or Article 3(2A) of the UK GDPR. To decide whether such processing activity is excluded requires consideration of the law relating to comity principles. We discuss this in [216] to [219] below.

196. It is implicit in our adoption of Privacy International's preferred construction that we reject Clearview's intersectional construction. Because Ms Proops' submissions were so focused on this proposed construction, we now explain why we were not persuaded by it.

Analysis of Clearview's proposed intersectional construction

197. Ms Proops sought to persuade us that her intersectional construction, which we have summarised at [131] to [133] above, was the only interpretation that gave meaning to all the words of Article 2(2)(a).

198. She characterised the language of Article 2(2)(a) as "widely framed", because it is not expressly limited to, for example, the national security activities of Member States. Had the EU legislators intended it to be so limited, Ms Proops said, they could and would have said so.

199. So, what was its purpose? As rehearsed above, Ms Proops said that since the bounds between the competence of the EU and the matters reserved to the national governments of its Member States were well-established, the purpose of Article 2(2)(a) could not have related to that issue. That would have no utility. Neither, she said, could its purpose be to exclude the processing activities of foreign states from the material scope of the GDPR, as Mr Pitt-Payne had argued, because that was a matter of public international law, and the EU would have no competence to regulate foreign states even if it wanted to. That too would have no utility.

200. This utility/futility argument is problematic for Clearview's case because, for its interpretation of Article 2(2)(a) to achieve the utility described by Ms Proops, the regulation by the EU of the processing in question must be something that is within EU competence and must not be something that comity principles preclude it from regulating as a matter of public international law (whether by any statutory provision or by application of common law principles). Otherwise, Clearview's reading of the provision makes it at least as futile as Ms Proops argued it would be on either the ICO's or Privacy International's preferred interpretations.

201. Clearview's construction requires, therefore, that the purpose of the EU legislators was to shield from EU regulation the processing of personal data that public international law would permit the EU to regulate. In other words, for reasons of comity they made a policy choice to go further than comity principles required. We can find no support in the language of the GDPR for the EU legislators having had such a purpose.

202. Ms Proops sought to persuade us that Article 2(2)(a) must have been intended to deal with the situation of foreign data processors who are not themselves foreign states, but whose processing is so intertwined with their clients' "quintessentially state activities" that to seek to regulate them would be deeply offensive to comity principles and would amount to regulation of foreign states "by the back door".

203. Ms Proops explained to us that a client's uploading of a 'probe image' initiates a search of Clearview's databases, and conditions the delivery of search results by Clearview (i.e., the facial images with vectors which most closely match the vectors of the probe image, together with any additional information collected in relation to those images). Ms Proops said that at this point Clearview's processing is, on any common-sense view, processing "in the course of" its clients' discharge of their state functions. That is because Clearview's processing intersects "perfectly and completely" with its clients' processing such that the client's processing in uploading the probe image and Clearview's processing in searching its databases and delivering the search results, are "two sides of the same coin".

204. We spent time at the hearing seeking to understand Clearview's case on intersectional construction, and we are grateful to Ms Proops for her patience in answering our questions. We struggle to see why it would be appropriate to focus exclusively on the moment in time that data is transferred between Clearview and its client in the way that Ms Proops proposed, when there was clearly processing of data happening both before (Clearview's Activity 1

processing) and after (the client's use of the data in furtherance of its national security and/or law enforcement functions) the moment upon which the intersectional analysis fixed. It is unclear to us why the focus should only be on the moment when data was transferred between Clearview and its client.

205. Ms Proops accepted that ample processing took place by Clearview prior to the client's uploading of a probe image. She accepted that there was no intersectionality there, but argued that because of the nature of the processing (i.e. it being 'Activity 1' processing only), it could not bring Clearview within the scope of the GDPR because on Clearview's construction of Article 3(2)(b) (which we discuss in [264] to [275] and [307] to [320] below) that processing involves no behavioural monitoring.

206. Ms Proops also acknowledged that after the moment of transfer of the search results data, a client might carry out further processing of the data that might involve behavioural monitoring, but she maintained that, if it did, Clearview would no longer be "on the field". It would play no part in any such behavioural monitoring, would have no control over it, and indeed it would have no knowledge of it. Those are points we grapple with in [346] to [351] below.

207. The temporal issue aside, we also struggle to see why the client's transfer of the probe image data to Clearview's system, and Clearview's transfer of the search results to its client, were otherwise "inextricably intertwined" except in the sense that both parties' activities were part of a common transaction (seeking a "match" between the client's probe image and images on Clearview's databases).

208. We do not see how the client's activities and Clearview's activities can be said to be "merged" at the point of transfer as Ms Proops suggested that they were. Our understanding is that use of the Service involves Clearview and its client each undertaking a distinct and separate task, and they carry out those tasks sequentially. The process necessarily starts with the client uploading a facial image to Clearview's system. That upload initiates a search of Clearview's system by reference to the facial vectors associated with the library of images stored in its databases, and the generation and transfer of a report of any search hits to the client. Clearview is not involved in the upload of the probe image, and the client is not involved in the searching of Clearview's databases or the production of the report. The output is ultimately the product of a common endeavour, and that output cannot be achieved by either party alone, but the roles of the parties to the transaction remain distinct. They cannot properly be said to be "merged".

209. Ms Proops argued her intersectional construction was "obvious" and applied as a matter of "common sense". It is not, however, an obvious construction, since it focuses on one moment of processing to the exclusion of many others, without explanation of why that should be so. When asked by the panel to clarify the mechanism by which Clearview and its clients' processing became so "inextricably intertwined", Ms Proops could only repeat that the parties' processing represent "two sides of the same coin", they "perfectly and completely intersect", and they are "merged" in the moment of exchange of data. The use of these amorphous concepts did not assist us in the exercise of statutory construction. The relationship between the activities of Clearview

and the activities of its clients are no more "merged" or "fundamentally intersected" than the activities of parties to any transaction that involves transfers between them of electronic data.

210. Although she argued that Clearview's processing was inextricably intertwined with the processing of its clients while they were exercising their state functions, Ms Proops accepted that foreign states could exercise their state functions without using Clearview's service (and without interference from the ICO). She argued that regulation of Clearview's service would amount to "back door" interference with foreign states' discharge of their state functions because it would have the effect of compelling them to change the way they discharge their functions. Employing her "two sides of the same coin" metaphor, Ms Proops said that regulating Clearview's side of the coin involves a reshaping of the tool in the hands of Clearview's foreign state clients in a way that is profoundly offensive from a comity perspective.

211. Ms Proops sought support from ***Google v CNIL*** (discussed above at [106] to [114] and at [165] to [167]), but that case was not about state activity, and neither was it about whether the processor was in territorial scope. As we have noted, Google was within the territorial scope of both the 95 Directive and the GDPR because it had an "establishment" in France (see [52] of ***Google v CNIL***). We note the CJEU confirmed at [58] of its judgment that it considered the EU legislature had competence to impose an obligation on a search engine to de-reference across all its search engines. The CJEU's decision in ***Google v CNIL*** turned on its interpretation of the substantive provisions about de-referencing, which it did not consider evinced an intention to confer a scope on the rights enshrined in those provisions that went beyond the borders of the territory of the Union. By contrast, the wording of Article 3(2)(b) GDPR expressly provides for extra-territorial effect.

212. While at times Ms Proops claimed Clearview's intersectional interpretation to be "obvious" and a matter of "common sense", she also made the less ambitious submission that it was "linguistically possible". Because it was "linguistically possible", she argued, it must be preferred because of the need to interpret the provision purposively and because of the principle of close confinement, which required the narrowest possible interpretation of the extent of the provision's extra-territorial effect. Ms Proops insisted that, given the role already played by the Treaties that establish the bounds of competence of the EU and the rules of public international law, the purpose of the provision was to prevent "back door" regulation of foreign states through regulating those who are not foreign states but who process data in the course of foreign state functions.

213. For the reasons explained in [160] to [162] above we do not accept the argument that, even where the legislator has indicated expressly that it intends a provision to have extra-territorial effect, the extent of any such extra-territoriality must be interpreted strictly such that the narrowest possible reading must be given to it. We have engaged in a purposive interpretation. Applying that purposive interpretation, we consider that Article 2(2)(a) means what Privacy International says it means. Neither the words of the provision, nor the words of the relevant recitals, provide any indication that Article 2(2)(a)

might have been enacted for the purpose suggested by Clearview, nor any suggestion that the legislators intended the words "in the course of" to bear the meaning for which Ms Proops argued.

214. For all of the reasons set out above, we reject the intersectional construction put forward by Clearview.

Alternative analysis based on the ICO's construction

215. If we are wrong to accept Privacy International's construction, and if Article 2(2)(a) deals not only with relations between the Union and its Member States, but also with other matters that the legislators saw fit to exclude from the scope of regulation out of respect for comity principles, we agree with both Mr Pitt-Payne and Ms Demetriou that this makes no material difference to the outcome of the appeal. We agree that these different approaches represent "different paths up the same mountain", both ultimately turning on what established comity principles prevent the EU (or in respect of the UK GDPR, the UK) from regulating.

Would regulation of Clearview's data processing breach comity principles?

216. As discussed in [62] to [71] above, the law provides for immunity applying not only to states but also to "separate entities", which may be private companies.

217. However, we have been directed to no specific authority for the proposition that any species of comity principle extends more generally to provide immunity to a private company providing a service to a state body, even in the course of "quintessentially state activities" such as national security or criminal law enforcement, where those services are provided independently on a commercial basis, and not as a servant or agent of the state, or otherwise in exercise of sovereign authority. While Ms Proops placed some emphasis upon the Court of Appeal's decision in ***Koo***, in that decision, state immunity was found to apply on the basis of an agency relationship between the bullion bank and the central bank, as we explained earlier. The case affords no support for the proposition that state immunity may apply to a private company that is neither the servant, nor the agent, of the body with sovereign authority. Insofar as Ms Proops also drew attention to Lord Sumption's reference in ***Belhaj*** to this being a "subject matter immunity", we have explained the context in which this was said at [65] above.

218. Ms Proops disavowed any suggestion that Clearview was itself carrying out state activities, that it should be treated as if it were a state body, or that it should be considered to be "standing in the shoes" of its clients. Neither did she claim Clearview to be the servant or agent of its foreign state clients. Indeed, the way Ms Proops put Clearview's case on whether its processing was "related to" behavioural monitoring by its clients for the purposes of Article 3, placed substantial emphasis on Clearview's independence from its clients.

219. Rather, Ms Proops argued Clearview's case on the basis of her intersectional construction of Article 2(2)(a). She reasoned that this was intended to exclude operators in situations like Clearview's from the scope of regulation out of an abundance of respect for comity principles, rather than because public

international law demands it. As explained above, we reject that intersectional construction.

Article 3(2)(b) GDPR: territorial scope

Our approach to the construction of Article 3(2)(b)

220. Clearview accepts that Article 3(2)(b) was intended by the legislature to afford the GDPR some degree of extra-territorial effect but says the FTT erred as to the nature and extent of that extra-territoriality.

221. Ms Proops argued that, looked at in the round, it is clear that Article 3 was not intended to achieve a wide and loose extra-territorial effect, but rather it was intended to remain significantly territorially focused. She submitted that Article 3(2) is the only "genuinely extra-territorial" provision in Article 3, Article 3(1) being about "conventional 'boots on the ground' territoriality" and Article 3(3) being about "UK outpost territoriality". Ms Proops characterised even Article 3(2) as being "territorially anchored", and indicative of an "avid desire" on the part of the EU legislators to avoid "exorbitance of approach" demanding that the degree of extra-territorial extent for which Article 3(2) provides, should be construed narrowly.

222. Both Clearview and the ICO pointed out that when the EU enacted the GDPR, it was clearly aware of the risks posed by large scale processing of personal data (as is clear from Recitals 6 and 7). Ms Proops argued that, while it would have been open to the legislators to legislate much more broadly, they chose to exercise restraint due to their wish to avoid affronting international comity principles. She said the practical result of this was that the GDPR was not intended to provide "all singing and all dancing" protection for data rights. Instead, it permits, without regulation, significant foreign processing operations that substantially engage the privacy rights of millions of EU data subjects, just as foreign state mass surveillance activities are excluded from regulation under international law. Ms Proops argued that this was simply the price that had to be paid to ensure that the protection of the interests of EU data subjects did not come at the expense of the protection of international comity.

223. Ms Proops argued that the degree of extra-territorial effect provided for by Article 3(2)(b) falls to be construed narrowly in line with the principles established by ***Al-Skeini*** and ***KBR***, and with wider comity principles. Because of the particularly weighty and onerous nature of the GDPR regime, and because of the need for legal certainty and proportionality, the need for "close confinement" in interpreting the extent of extra-territoriality in the context of the GDPR is, Ms Proops argued, even greater.

224. Ms Proops warned against treating data rights as a "trump card" that overrides other policy considerations, cautioning that concerns about comity, utility, certainty and proportionality must be given due weight. She referred us to a variety of authorities dealing with the construction of different legislative schemes with a view to demonstrating that even when there was a legitimate underlying protective purpose to legislation, that did not necessarily justify a broad construction.

225. In ***R (Black) Secretary of State for Justice*** [2017] UKSC 81, [2018] AC 215 (***"Black"***) the Supreme Court considered whether legislation banning smoking in public places in the UK applied to the Crown. It held that there was a presumption against legislation applying to the Crown unless such application was expressly provided for, and because the smoking ban legislation included no provision to that effect, it did not bind the Crown. The practical effect of this was that the smoking ban did not apply in UK prisons, so prisoners, staff and visitors would not be protected from the effects of passive smoking. Even though the policy driver for the legislation was a very important one (to protect public health by preventing passive smoking in public places) that was not enough, the Justices decided, to justify a broad interpretation that the Crown was bound by it.

226. Ms Proops said that, by analogy, Article 3(2)(b) GDPR should not be given a broad interpretation to bring third party controllers who do not engage in behavioural monitoring, within the scope of regulation, even though that might produce an optimal result in terms of the protection of the data rights of EU data subjects. Ms Proops argued that to extend the reach of regulation to such persons would be unduly exorbitant, because the policy intent can be achieved by capturing only those "doing the mischief" at which the provision is aimed, namely the behavioural monitoring of EU data subjects.

227. As explained at [160] to [162] above, we are not persuaded that ***KBR***, ***Al-Skeini*** or any of the other authorities to which our attention was directed, establish a general proposition that where words in EU legislation are capable of bearing more than one meaning the meaning that results in the least degree of extra-territorial effect must be applied, even if the usual rules of statutory construction would favour a different meaning.

228. We do not accept the narrow interpretation that Ms Proops proposes. While we infer that the EU legislators intended to respect comity principles, and we factor that intention into our interpretation of these provisions, we reject the notion that we are compelled to accept the reading that gives the provision the least degree of extra-territorial extent provided that such a reading is "linguistically possible", however unlikely. Instead, we take a conventional purposive approach to the construction of the GDPRs.

What was the policy objective behind Article 3(2)(b)?

229. Clearview's case on the construction of Article 3(2)(b) is that it is clear on its face that the legislature's aim was to capture intrusive behavioural monitoring where the sights of the person doing the behavioural monitoring are trained on the behaviours of EU data subjects in the EU. It is the behavioural monitoring activity, and the intrusion that results from that activity, that is the "mischief" the legislators sought to tackle.

230. This understanding is consistent with the ICO's case, as expressed in his Skeleton Argument at [167]):

> "The point of 3(2)(b) is to ensure that EU data subjects have protection against being monitored by processing of their personal data. Having one's behaviour monitored is inherently objectionable and merits protection."

231. Ms Proops submitted that once one appreciates the mischief the provision is aimed at is the monitoring, it becomes clear that Article 3(2)(b) must be construed to apply to the *person doing the monitoring*, and therefore responsible for the mischief. Regulating the person doing the monitoring means, Ms Proops says, that you "hit the policy nail on the head".

232. Ms Proops invited us to look to the Travaux in respect of the GDPR as an aid to construing Article 3(2)(b), citing ***Pickering*** (see [115] above) as confirming the Court of Appeal's approval of such a practice. She suggested the Travaux tell a clear story that is consistent with Clearview's case that the legislators' focus was always on capturing *the person actually engaged in the monitoring.* She took us to the Commission's 2012 impact assessment which discussed different options for data reform where it appeared to contemplate the data controller and the person monitoring the behaviour being one and the same. A similar passage appears in the 2016 Commission communication to the European Parliament. We have set out the respective texts, italicising the passages that Ms Proops relied upon at [117] to [118] above.

233. Ms Proops said that these passages in the Travaux support her narrow interpretation of Article 3(2)(b). She argued that had the legislators envisaged the scope of regulation extending to companies outside the Union monitoring the behaviour of EU data subjects within the EU (and those who service such companies), *who are not themselves engaged in behavioural monitoring*, they would surely have said something about such a significant extension of extra-territorial regulation.

234. Mr Pitt-Payne maintained that the Travaux relied upon by Clearview were of little assistance. He said that the two passages referred to are simply brief statements that do not directly address the question in issue in the appeal, namely whether Article 3(2)(b) applies to a single party situation or a multi-party situation. He argued that the Travaux did not rule out a multi-party situation.

235. Having read the Travaux, we observe that the Commission's 2012 impact assessment is a relatively brief, high level explanation of different options for regulation, produced some years before the GDPR was legislated. The focus of the Commission's subsequent communication to the European Parliament was on the transfer and exchange of personal data between the EU and the US. The purpose of the communication was to confirm what had happened since a 2013 communication on rebuilding trust in EU-US data flows. One element of that was the data reform package that would become the GDPR. The wording about territorial scope is, again, in the nature of a high level explanation. The wording relied on by Ms Proops amounts to individual sentences within high level explanations. For these reasons, we consider they are of limited significance.

236. The ICO relied on the EDPB Guidelines. We have set out the material parts at [119] above. Having read these in detail, we note that they focus directly on Article 3 and the territorial scope of the GDPR. The introduction to the EDPB Guidelines explains that the territorial scope of the GDPR represented a significant evolution of EU data protection law compared with the previous framework in the 95 Directive. The introduction explains the purpose of the

EDPB Guidelines as being to ensure a consistent application of the GDPR about territorial scope, and that they set out, and clarify, the criteria for determining the application of territorial scope.

237. While Ms Proops commended the Travaux as a more reliable aid to construction than the EDPB Guidelines upon which the ICO relied, we note that the Court of Appeal said in ***Soriano*** that the EDPB Guidelines are relevant to the exercise of construction, albeit not binding (see [101] above). We approach the EDPB Guidelines in the spirit suggested by the Court of Appeal in ***Soriano***, and we have found them to be of assistance. As explained above, they are directed expressly at the question of how territorial scope of the GDPR is to be interpreted, and applied, both within and outside the EU.

238. At page 20 of the EDPB Guidelines in the section headed "d) Processor not established in the Union" it is stated:

> "The EDPB considers there needs to be a connection between processing activity and the offering of good or service, but both processing by a controller and a processor are relevant and to be taken into account."

239. Further, Example 20, set out at page 21 of the EDPB Guidelines, concerns a distinct processor and controller.

240. Ms Proops dismissed this example on the basis that it lacked equivalence to Clearview's situation because, while it was right that an agent of a controller acting on behalf of that controller and subject to the controller's direction would fall within the scope of regulation, the same should not apply to an independent third-party controller like Clearview. This was especially so, Ms Proops argued, because, as a result of the limited functionality of the Service, Clearview had no insight into the onward use of the data it supplies to its clients, with the consequence that it cannot know in any particular case whether any of its clients have ever used the data acquired via the Service to monitor the behaviour of any data subject in the UK. We accept that there are factual differences between Example 20 and the present case. Nonetheless, it provides a clear instance of a situation where activities undertaken by one party (the processor) are said to come within Article 3(2)(b) on the basis of their relationship to the behavioural monitoring carried out by another party (the controller).

241. While we agree with Ms Proops that the policy objective behind Article 3(2)(b) was to address the "mischief" of behavioural monitoring, and the intrusiveness that results from such monitoring, we are not persuaded that it was aimed *only* at the controller *conducting* the behavioural monitoring.

The meaning of "related to" in Article 3(2)(b)

242. We heard a substantial amount of argument about the meaning of the words "related to" in Article 3(2). They are everyday words, and our starting point is their natural meaning, which is to denote a relationship of connection or association between two or more things.

243. Mr Pitt-Payne argued that as the EDPB Guidelines indicate that one can have a situation where a processor's activities are related to monitoring by a controller, one can equally have a situation where processing by one controller

is related to monitoring by another controller. Mr Pitt-Payne submitted that Article 3(2)(b) should be interpreted to include this situation.

244. Ms Proops argued that, because the stem phrase "related to" in Article 3(2) applies to both paragraph (a) which concerns the offering of goods and services to data subjects in the Union, and paragraph (b) which concerns monitoring of behaviour within the Union, its meaning must be the same in relation to both limbs. She said that, because it is clear that in (a) the only controllers who are caught are the people offering goods and services into the Union, it must follow that paragraph (b) can only catch controllers who are the people actually doing the behavioural monitoring.

245. We do not agree. The fact that paragraphs (a) and (b) proceed from the same stem does not mean that "related to" describes the same relationship or connection in both sub-paragraphs. Rather, in each instance, "related to" indicates that there is a relationship or connection (between two or more things) and each relationship is then defined by the respective wording in the two sub-paragraphs that follow.

246. Ms Proops directed us to the principle described by Lord Hutton in ***R v Kansal (No. 2)*** [2002] 2 AC 69 (at [102]) (***"Kansal"***) that where Parliament uses words in a statute it is to be presumed that 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. We accept that principle, but a reading of Article 3(2) to the effect that sub-paragraphs (a) and (b) deal with different relationships does not prevent the words "related to" from having a consistent and coherent meaning, so it does not offend against Lord Hutton's principle in ***Kansal***.

247. We note that the EDPB Guidelines are not consistent with this part of Ms Proops' interpretation. See [238] to [241] above, and also page 21 of the EDPB Guidelines, which explains that for a data processor not established in the Union, it is necessary to look at whether the processing activities by the processor are related to the targeting activities of the controller. As we have noted, these examples highlight that a processor can be caught by Article 3(2)(b) where its processing is related to the actions of a separate data controller.

248. Ms Proops encouraged us to read the words "related to" as serving two functions where they appear in relation to Article 3(2)(b):

    a. a narrowing function, ensuring that the wider, unrelated, processing carried out by the controller doing the behavioural monitoring is not caught; yet also

    b. an expansive function, making clear that where a controller is engaged in relevant behavioural monitoring, their "related processing" is included, such as preparatory acts that do not amount to monitoring but are a fundamental part of the behavioural monitoring exercise.

249. We did not find this to be a natural or desirable approach. Had the legislators intended a narrowing of the scope of Article 3(2)(b) this could have been achieved simply by omitting the words "related to" altogether, and referring, instead, to "the monitoring of their behaviour".

250. Again, we note that neither the wording of the provision, nor the examples in the EDPB Guidelines, support Ms Proops' favoured interpretation of Article 3(2)(b). The EDPB Guidelines confirm the importance of assessing monitoring, which they explain implies the controller has a specific purpose in mind for the collection and subsequent reuse of the relevant data about an individual's behaviour in the EU. It is necessary to consider the controller's purposes for processing the data and any subsequent behavioural analysis or profiling techniques involving that data (see page 21 of the EDPB Guidelines). The EDPB Guidelines indicate that where this is confirmed to amount to monitoring, the test is whether the processing relates to it. Example 18 explains that a processor in the US that optimises and maintains an app designed by an app developer (in Canada) to monitor the behaviour of data subjects in the EU, will be caught by Article 3(2)(b).

251. Ms Proops accepted that the language of Article 3(2)(b) was sufficiently flexible to make the reading advocated by Mr Pitt-Payne "tenable", and ultimately conceded that if the proper construction turned on an ordinary linguistic interpretation of the provisions, Clearview would be in "grave difficulty". She argued, however, that because of the principle of "close confinement" that falls to be applied when considering extra-territorial effect (see [155] to [162] and [170] to [175] above), and because of the four imperatives of comity, utility, certainty and proportionality (discussed in [155] to [178] above), we could only adopt Mr Pitt-Payne's (and the FTT's) reading if we were compelled to do so because there was no other tenable reading.

252. For the reasons set out in the preceding paragraphs, we do not agree that this is the proper approach. Instead, we approach the construction of Article 3(2)(b) on the basis that it expressly provides for extra-territorial effect. As such, while our construction is informed by our inference that the legislators would have intended to respect comity principles, we apply the ordinary rules of statutory construction to determining the extent of its extra-territorial effect. There is no requirement for us to interpret the words artificially so as to restrict the extent of the provision's extra-territorial effect as far as the words can linguistically bear. To do so would frustrate the legislators' intent.

253. In ***Soriano***, at [100], Warby LJ acknowledged the words "related to" can bear different interpretations, and he applied an expansive meaning to them in relation to Article 3(2)(a), such that the data subject whose data is processed need not be the same person as the offeree of the goods or services:

> "The language could be read as indicating a legislative intention to ensure 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 is not the position here. But the case has never been argued on that basis, so I approach the issue – as everyone appears to have done so far – on the footing 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, providing the two activities are "related to" one another."

254. Just as Warby LJ gave the words "related to" in Article 3(2)(a) an expansive meaning, we have given them an expansive meaning in Article 3(2)(b). We

read Article 3(2)(b) as applying, not only to controllers who themselves conduct behavioural monitoring, but also to controllers whose data processing is related to behavioural monitoring carried out by another controller. The words "related to" require a relationship between the processing of the individual's personal data and the monitoring of the behaviour, and there is (as the FTT was entitled to find) "such a close connection between the creation, maintenance and operation of the Database and the monitoring of behaviour undertaken by the clients that Clearview's processing activities are related to that monitoring" (see [143] and [144] of the FTT's decision).

255. Furthermore, we consider that our reading of Article 3(2)(b) is also consistent with the wording in the EDPB Guidelines, which we have considered on the basis that ***Soriano*** confirmed them to be relevant to the construction of Article 3.

The meaning of "behavioural monitoring" in Article 3(2)(b)

256. We also heard extensive submissions as to what amounts to "behavioural monitoring" for the purposes of the GDPRs. As the FTT pointed out in its decision, there is no definition in either of the GDPRs of "behavioural monitoring".

257. Mr Susskind, for the ICO, said Clearview's mass collection of data (via deployment of its "crawlers" to search the public facing internet for "every single picture that exists of every single person", collecting those images, together with other personal information from the websites on which the images are found), and its ordering of that data by mapping it, assigning vectors, and arranging the data according to similarity of facial vectors, must itself amount to behavioural monitoring so as to engage Article 3(2)(b). He said this was the way the ICO put his case before the FTT, but the FTT misunderstood it and mischaracterised his case at [129] of its decision, wrongly focusing only on the gathering of the facial vectors and the indexing of the data according to the similarities in those vectors, which in fact represents only a part of Clearview's Activity 1 processing.

258. He drew our attention to Recitals 6, 7 and 24 (set out in [53] above) which explain the backdrop to the GDPR, and which Mr Susskind said should inform our understanding of the term "behavioural monitoring".

259. Recitals 6 and 7 establish the GDPR as a response to the challenges posed by the new scale of collection and use of personal data, including by private companies, in the modern world. It is a regime born in the age of "Big Data" and designed to address its challenges. Mr Susskind encouraged us to interpret the GDPRs in a way that reflects that legislative purpose, and does not undermine it.

260. Mr Susskind also took us to Recital 24, the opening sentence of which traverses the terms of Article 3(2)(b), before giving guidance on what amounts to "behavioural monitoring".

261. Mr Susskind encouraged us to take from this Recital not only that it provides an example of an indicator of behavioural monitoring (i.e. whether a natural person is being tracked on the internet), but also indicates that where there is

"*potential subsequent use* of personal data processing techniques" it is not necessary for there to be actual profiling for the definition of "monitoring behaviour" to be engaged.

262. He highlighted that Clearview's crawlers search the public-facing internet (or in the case of proprietary crawlers, search the platforms which they are deployed to search) on an indiscriminate and almost constant rolling basis. Once they have collected a facial image of a natural person, assigned it vectors, sorted it and stored it, the crawlers do not stop there. They continue scraping the internet for other facial images and will collect, map, sort and store further images, including images of the same individual, as and when they are encountered with the result that for every person whose image has been scraped, mapped, sorted and stored, there may well be a collection of multiple images captured at different times and in different contexts, together with associated personal data collected from the webpages from which the images were collected, which information the FTT found to be "behaviourally rich". While the crawlers are deployed to collect facial images to which they can assign vectors, the data collected goes far beyond facial images.

263. Mr Susskind said these images tell stories of where people work, what they like, what they dislike, with whom they associate, their family and friends, their interests and their history. He submitted that this must, on any common sense view, amount to "behavioural monitoring", and was precisely the kind of activity that the legislators intended to catch when they enacted the GDPRs.

264. Ms Proops argued that for an activity to amount to behavioural monitoring there must be more than simply the mass harvesting of data and its sorting and indexing by person: the data had to be further analysed or interrogated or otherwise utilised in some way. For this proposition, she placed reliance on the Court of Appeal's decision in ***Soriano***.

265. However, ***Soriano*** is not authority for all that Clearview requires of it. While Warby LJ said (at [103]) that the mere fact that the defendants in that case had created a collection of personal data related to the claimant's behaviour "might not" be sufficient to amount to behavioural monitoring, he did not say that it could never be sufficient, and he said it was "arguable" that the activities of assembling, analysing, sorting and reconfiguring such data, and then publishing the result in articles, did fall within the meaning of "monitoring" and within the scope of the EDPB's notions of "behavioural analysis and profiling". We also accept Mr Susskind's submission regarding the relevance of "potential subsequent use" of the personal data as indicated in Recital 24. In this regard, we note that the discussion at page 20 of the EDPB Guidelines also places emphasis on the subsequent use of the data.

266. Mr Susskind maintained that Ms Proops' interpretation of "behavioural monitoring" was predicated on an interpretation of behavioural monitoring that required the monitoring to be "active", and there was no warrant for such a requirement either in the wording of the GDPR or in what the Court of Appeal said in ***Soriano***. Mr Susskind argued that monitoring could just as well be a "passive" affair. He gave the example of a hotel placing a CCTV camera in its lobby, and leaving it to record the comings and goings of staff, residents and members of the public. The making of such a recording must, Mr Susskind

said, amount to monitoring the behaviour of natural persons, and this is so even if no one ever watches the recording or subjects it to any analysis.

267. We agree that the making of a recording in the circumstances Mr Susskind describes must amount to behavioural monitoring, regardless of whether the recording is ever accessed. What is important is not that the recording is accessed, but that it is made with a view to it being available to be accessed in the future should that be needed, consistent with the assessment of whether it amounts to behavioural monitoring reflecting the "potential subsequent use of personal data processing techniques which consist of profiling a natural person" (per Recital 24).

268. Ms Proops' "active" understanding of behavioural monitoring is also somewhat at odds with the EDPB's citing of "online tracking through the use of cookies" (at page 20 of the EDPB Guidelines) as an example of monitoring in the digital age.

269. Ms Proops argued that Clearview's data collection and sorting activities could not amount to "behavioural monitoring" because the data was not sorted and indexed by reference to behaviour. We consider this argument to be misconceived because if one is interested in monitoring the behaviour of natural persons, one does not organise the data by reference to the behaviour it reveals, but rather by the identity of those whose behavioural data has been collected. It is Clearview's capability for identifying individuals that makes its Service such an ideal tool for behavioural monitoring.

270. The ability to map internet images of an individual's face and assign unique vectors to them facilitates the efficient mining of Clearview's extensive database. A Clearview client could have an image of a person's face, with no name, and no other information about them. Clearview's data collection and sorting means that it might have pulled together a substantial amount of behaviourally rich information about that person, which it argues is highly likely to be accurate about them (because the information has been sifted and stored by reference to unique facial features that are turned into digital vectors).

271. The EDPB Guidelines say that the word "monitoring" implies that the controller has a specific purpose in mind for the collection and subsequent reuse of the data about an individual's behaviour within the EU, and they say that when considering whether processing involves the monitoring of a data subject's behaviour, the controller's purpose for processing the data and potential subsequent use of profiling techniques are relevant considerations (see page 20 of the EDPB Guidelines).

272. While Ms Proops was somewhat coy about what Clearview's clients might do with the search results they receive from Clearview, it is apparent from the 'Lunch and Learn' marketing materials that Clearview put into evidence that the Service was marketed as a valuable tool both for identifying, and for learning about, individuals in a way that can significantly assist national security and criminal law enforcement investigations. The further use, interrogation and analysis to which the data is subjected by Clearview's clients does not indicate that the behavioural monitoring occurs only after Clearview has transmitted the search results to the client. Rather, before a client even

submits a probe image, 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. This information will already be contained and arranged within the Service even if a probe image of that individual is never submitted by a client. This, together with the potential for further use of it by Clearview's clients, further strengthens the case for Clearview's Activity 1 processing amounting to behavioural monitoring (per page 20 of the EDPB Guidelines).

273. There is force in Mr Susskind's argument that the language Ms Proops used in her submissions about monitoring having to be active or watchful in terms of it needing to demonstrate "looking at", "watching, "scrutinising", and "learning", was apt to mislead. This is language about what humans do, but "monitoring" for the purposes of the GDPRs is not confined to that. Mr Susskind submitted that at the stage when Clearview gathers information about people, this does not require a person to sit down and trawl the internet to find images: this is done digitally by Clearview's crawlers. Mr Susskind argued that, if "watchful" is stripped of its anthropomorphic connotations, the Clearview crawlers are actually extremely watchful. Their actions in crawling through a range of websites on a virtually constant basis, mean they will "watch" or "see" far more than any human could.

274. We agree with the ICO that Article 3(2) of the GDPR must be interpreted as a response to the challenges posed by the age of 'Big Data', which the Recitals show the EU legislators were keenly aware of and had in mind when deciding upon the terms of the regulation they were creating. It is important to approach the language of Article 3 with this in mind, and not to see it through the prism of analogue methods of monitoring and surveillance that require human involvement.

275. We therefore adopt a broad interpretation of the words "behavioural monitoring" that encompasses "passive" collection, sorting, classification and storing of data by automated means with a view to potential subsequent use (including by another controller) of personal data processing techniques which consist of profiling a natural person. It does not require active "watchfulness" in the sense of human involvement, it does not require analysis beyond automated sorting and classification with a view to subsequent future use, and it does not require the data to be sorted and classified by reference to subjects' behaviour.

<u>The Grounds of Appeal</u>

276. In the light of what we have decided about the proper construction of Articles 2(2)(a) and 3(2)(b) GDPR we can now deal with the ICO's grounds of appeal more succinctly.

Ground 1

277. Ground 1 raises the issue whether the FTT erred in law in finding that Clearview's clients were excluded from the material scope of the GDPR under Article 2(2)(a). The ICO argued two sub-grounds:

(1) the FTT erred by equating Clearview's private sector contractor clients with the foreign states to whom they were supplying services; and

(2) the FTT failed to distinguish between the activities of Clearview's private sector contractor clients relating to matters of national security and those relating to criminal law enforcement.

278. For the reasons explained in [141] and [144] to [147] above, we are unable to identify from its reasons how or why the FTT reached its conclusion that the exception from material scope in Article 2(2)(a) applied to Clearview's clients. As such, we cannot say whether they erred in the specific ways alleged by the ICO's two sub-grounds.

279. However, for the reasons set out above in [190] to [194] above, we accept Privacy International's construction of Article 2(2)(a) that the provision deals only with the division of responsibility between the Union and its Member States, and is not about foreign states or private bodies providing services to foreign states at all. From this, it follows that the FTT erred in law in finding that Clearview's clients' processing fell within Article 2(2)(a), so Ground 1 succeeds on that more general basis.

280. Having identified an error of law by the FTT, we must consider whether that error was material. We must therefore consider whether the FTT's conclusion that Clearview's clients were beyond material scope of the GDPR was correct, albeit for the wrong reasons. That requires consideration of whether the processing carried out by Clearview's clients was excluded from the scope of the GDPR by independent operation of public international law relating to comity principles.

281. It was agreed by the parties that the processing of Clearview's foreign state clients fell outside the scope of regulation.

282. In relation to the processing of Clearview's private sector contractor clients, Ms Proops relied heavily on the FTT's finding (at [146] of its decision) that those private sector clients each "carry out criminal law enforcement and/or national security functions, and use the Service in furtherance of those functions". She relied on this to support her argument that Clearview's private sector contractor clients are also beyond the scope of regulation by the GDPR, even if Clearview's intersectional construction is wrong, as we have decided it was (see [197] to [214] above).

283. Ms Proops characterised the statement at [146] of the FTT's decision as an "unequivocal finding of fact" based on the FTT's acceptance of Mr Mulcaire's evidence, that went unchallenged at the hearing before the FTT (even though Mr Pitt-Payne had the opportunity to cross-examine Mr Mulcaire).

284. Mr Pitt-Payne accepted the finding of fact to the extent that it speaks to the clients providing assistance to foreign states in national security and/or criminal law enforcement matters. He argued, however, that those findings were insufficient, on their own, to found a conclusion that the contractor clients' activities were carried out in exercise of sovereign authority and therefore attracted state immunity, or otherwise attracted protection from regulation by operation of comity principles as a matter of international law.

Such a conclusion could, Mr Pitt-Payne argued, only be reached based on findings of fact as to the specific tasks carried out by the contractor clients in the context of their national security and/or criminal law enforcement functions, and as to the specific terms of the relationship between the contractor and its foreign state client.

285. While Ms Proops argued that the ICO could not rely on Mr Pitt-Payne's failure to challenge Mr Mulcaire's evidence, Mr Pitt-Payne responded that it was not for the ICO to fill the gaps in Clearview's evidential case.

286. Ultimately, where a party seeks to challenge a penalty imposed by the ICO, the principles set out by the Court of Appeal in ***Doorstep Dispensaree*** apply (see [121] to [124] above), with the result that the burden of proof is on the party seeking to challenge the penalty. In respect of the question whether Clearview's private sector clients fell out of scope, the burden of proof therefore lay on Clearview to establish its case that they were.

287. The finding made by the FTT in paragraph [146] of its decision that "all of [Clearview]'s current clients carry out criminal law enforcement and/or national security functions and use the Service in furtherance of those functions", lacks specificity. If it amounts to a finding that those private sector clients carry out those activities in exercise of sovereign authority, the FTT's primary findings of fact upon which that finding is based are inadequate to support such a conclusion, and, importantly, we have not been directed to any evidence that was before the FTT that would have justified findings of fact that would support such a conclusion.

288. For these reasons we are satisfied that the error of law established by Ground 1 was material.

Ground 2

289. Ground 2 raises the issue whether the FTT erred in law in finding that Clearview itself was excluded from the material scope of the GDPR under Article 2(2)(a). For the avoidance of doubt, this is a free-standing ground of appeal that arises even if we are wrong to hold, as we have done immediately above, that there was insufficient evidence before the FTT to support a conclusion that the processing undertaken by Clearview's private sector clients falls outside the scope of regulation.

290. As we indicated earlier, the ICO argued four sub-grounds:

    (1) the FTT failed to have regard to the fact that the ICO's Notices were directed at Clearview's own processing and not its clients' processing;

    (2) the FTT failed to address Clearview's specific activities in the course of which its relevant processing took place (namely its "Activity 1" processing and its "Activity 2" processing);

    (3) the FTT reached a conclusion that involved reading Article 2 and/or Article 3 of the GDPRs as if additional wording had been inserted into them; and

(4) the FTT reached a conclusion that would lead to an obvious anomaly, and indeed absurdity, in the application of Article 2(2)(d), but disregarded this when interpreting Article 2.

291. Mr Pitt-Payne argued Ground 2 in broad terms as the FTT concluding, without proper explanation, that Clearview's own processing fell outside the material scope of the GDPR. Mr Pitt-Payne argued that even if the FTT was correct to conclude that Clearview's clients fell outside the material scope of the GDPR, it did not follow from this that Clearview's own processing also fell outside its material scope. At the heart of Ground 2 was the proposition that Clearview is not a foreign state, it is a private company, and nothing in the processing that Clearview itself carried out made it suitable only for being used in conjunction with state functions.

292. We have already decided, consistent with the arguments Privacy International put forward, that the words "outside the scope of Union law" in Article 2(2)(a) GDPR, relate to the division of responsibilities between the Union and its Member States: see [190] to [194] above. It follows from this interpretation that the FTT erred in law when it found that Clearview's own processing fell within the exception to material scope set out in Article 2(2)(a).

293. As with Ground 1, we have considered whether the FTT reached the right conclusion for the wrong reasons. For the reasons set out in [217] to [219] above we are satisfied that there was no basis in law for concluding that Clearview's own processing was beyond the material scope of the GDPR.

294. Accordingly, even if our construction of Article 2(2)(a) is wrong, and the ICO's construction that the wording applies to all matters that are without the competence of the Union, is to be preferred, this makes no practical difference because the same consideration of comity principles comes into play, whether in interpreting the words of Article 2(2)(a) or by independent operation of international law principles.

295. For completeness, we turn to Mr Pitt-Payne's four specific sub-grounds advanced under this Ground. We consider sub-grounds 1 and 2 overlap to a sufficient extent that it is appropriate to deal with both together. Both sub-grounds are about the adequacy of the FTT's reasoning to support its conclusion that Clearview's processing fell outside the material scope of the GDPR.

296. Mr Pitt-Payne argued that the FTT effectively assimilated processing by Clearview with processing by its clients and [154] of the FTT's decision effectively jumped without explanation from reasoning that Clearview's clients were outside the material scope of the GDPR, to concluding that Clearview's own processing was outside scope.

297. Ms Proops argued that the reasoning at [154] was concise but adequate, given that the FTT had made core findings about Clearview's clients and their functions. She argued that [154] amounted to a conclusion that Clearview's processing sufficiently intersected with its clients' state activities that it could be regarded as falling outside the scope of Union law. Ms Proops argued that the FTT's reasoning in [154] relied on cumulative reasoning, including at [146] and [147] of the decision. She argued that this had to be the case because no

one had argued that Clearview was itself performing state functions or stood in its clients' shoes (and it would have been misconceived to do so).

298. As explained at [218] above, Ms Proops confirmed that Clearview did not put forward its case below on the basis that its own processing was outside material scope as a result of Article 2(2)(a). Ms Proops explained that Clearview's case had been that its Service was used exclusively in furtherance of the discharge of foreign state functions but focused on the territorial lens of Article 3(2)(b) rather than the material scope lens of Article 2(2)(a).

299. We agree with Mr Pitt-Payne's arguments. We have already described the paucity of the FTT's reasoning on material scope at [141], and [144] to [147] above. [154] of the FTT's decision appears to recite the statutory position rather than explain a conclusion. As we noted earlier, the FTT started its reasoning at [154] with "*We have concluded for all these reasons*…". This suggests that there was earlier reasoning in the FTT's decision that went to this specific issue. We have, however, been unable to identify any clear reasoning by the FTT about what followed from the factual findings it made about Clearview's own processing activities that allowed it to reach that conclusion. While [155] of the FTT's decision appears to provide additional reasoning for the conclusion at [154], once again, the substance of that paragraph is addressed to what the FTT had decided about Clearview's *clients*, not Clearview itself.

300. Even if the FTT decided the appeal on the basis of an analysis that was not put forward by any of the parties, the reasoning the FTT provided did not address Clearview's own activities or explain how it concluded that they fell outside the material scope of the GDPRs.

301. We conclude that the FTT's reasoning focused substantially on the position of Clearview's clients, without addressing adequately why Clearview's own processing was found to fall outside scope.

302. Sub-ground 3 of Ground 2 is that the FTT reached a conclusion about the test for material scope that required reading into the provision additional wording to the effect that the processing by Clearview's clients must fall within the material scope of the GDPR before it can be concluded that Clearview's own processing can fall within it. We address this point in the context of Clearview's Additional Reason 2 in [331] to [344] below.

303. Sub-ground 4 of Ground 2 is that the FTT's analysis would create an anomaly or lacuna in the data protection framework. In summary, Mr Pitt-Payne's argument was that the FTT's construction of Article 2(2)(a) would, if applied to Article 2(2)(d) of the GDPR, result in an absurd outcome. If Clearview provided its services to a UK law enforcement body, that body would be outside the material scope of the GDPR under Article 2(2)(d). However, that body's processing of personal data would be regulated under the Law Enforcement Directive (see [60] to [61] above). Clearview would not, however, fall within the definition of a competent authority and therefore its processing would not be regulated at all.

304. In light of the clear conclusion we have already reached on the broader issue of what Article 2(2)(a) means, we do not consider it necessary to reach a particular conclusion about this alleged absurdity.

305. We have therefore decided that the FTT made material errors of law in:

    (a) its application of Article 2(2)(a) in concluding that Clearview's own processing must fall outside the material scope of the GDPR as a result of its clients' activities and, to the extent that it did reach a conclusion that Clearview's own processing fell out of material scope on some other basis; and

    (b) the adequacy of its reasoning to explain that conclusion.

    That decision is supported by our explanation why there was no basis in law for concluding that Clearview's processing was beyond the material scope of the GDPR.

Ground 3

306. Ground 3 raises the issue whether Clearview itself undertakes behavioural monitoring of UK data subjects within the meaning of Article 3(2)(b) GDPR.

307. The FTT found that, while Clearview's processing facilitates the efficiency of the Service and is processing that is "related to" behavioural monitoring by its clients, Clearview does not itself undertake monitoring of UK data subjects within the meaning of Article 3(2)(b) GDPR (see [129], [143] and [144] of the FTT's decision).

308. At the hearing, Mr Susskind articulated the ICO's case somewhat differently from the way it was put in the ICO's skeleton argument. Looked at overall, he identified the following respects in which he said the FTT had fallen into error:

    a. the FTT erred in its understanding that intentionally gathering behavioural data about a natural person could never be sufficient to amount to behavioural monitoring, as it involved automated monitoring and something further is required such as analysis or interrogation;

    b. the FTT erred in assuming that if further analysis or interrogation were needed, it would have to be done by Clearview for Clearview to be engaged in behavioural monitoring;

    c. the FTT misunderstood the ICO's case and wrongly focused only on the gathering of the facial vectors created from the personal data scraped from the internet and the indexing of the images according to those facial vectors;

    d. the FTT erred in deciding that Clearview's organising and cataloguing of the data it had scraped from the internet did not itself amount to behavioural monitoring; and

    e. the FTT erred in importing into its assessment of whether Clearview was engaged in behavioural monitoring anthropomorphised concepts

such as “watchfulness” that are inappropriate to an analysis of digital surveillance.

309. In terms of the first of these points, Mr Susskind argued that while Warby LJ observed in ***Soriano*** (at [103]) that mere gathering of behavioural data about a natural person “might” not be enough to amount to behavioural monitoring, nothing in ***Soriano*** precludes the possibility that it might be enough in some circumstances.

310. While it is true that Warby LJ does not go as far as to rule out that proposition entirely, we accept that he does not appear to consider it likely, and the text at page 20 of the EDPB Guidelines also does not support the proposition that the mere gathering of behavioural data will itself amount to behavioural monitoring. However, that is not by any means determinative of whether Clearview engages in behavioural monitoring because, as the FTT found, Clearview does a lot more than simply gather data: it gathers it, analyses it, sorts it and stores it, and it does so with a view to permitting clients to upload images to the Service to initiate a search of the database and potentially to engage in further processing in furtherance of their national security and/or criminal law enforcement functions. To the extent that ***Soriano*** requires “something further” in the nature of analysis, the FTT’s findings of fact (see [112] to [114] of the FTT’s decision) establish that Clearview engages in analysis, albeit without human involvement.

311. Clearview’s processing is digital, automated and passive. It is achieved by applying algorithms to the collected data and it involves no human intervention. Ms Proops told us that no one at Clearview is able to “see” the data, but there is nothing in the wording of Article 3, in the Recitals or in the EDPB Guidelines that indicates any requirement for “seeing” or “watching” to establish that monitoring is taking place.

312. As the example of CCTV surveillance we discussed at [266] to [267] above demonstrates, monitoring may occur as soon as a camera is switched to “record”. One does not have to wait until the recording is viewed for it to amount to monitoring, and it may amount to monitoring even if the recording is never viewed. The key to establishing monitoring is not that someone or something actually accesses the output; it is that the data is available to be accessed should access be needed, and the data has been gathered in contemplation of that potential eventuality. As we discussed at [260] to [275] above, Recital 24 and the EDPB Guidelines assist in highlighting the relevance of the controller’s purpose in processing the data and the relevance of the potential subsequent use of the data, including its use by another.

313. Turning to Mr Susskind’s second point, there is considerable overlap with what we have already discussed in relation to the first alleged error. In dismissing the ICO’s “indexing case” on the basis that Clearview’s processing “in itself reveals nothing about the behaviour of a person” (see [129] of the FTT’s decision), the FTT failed to factor in the two matters that Recital 24 and the EDPB Guidelines indicate are relevant:

    a. what it found to be Clearview’s purpose in processing the data:

> "The whole purpose of the processing of data by [Clearview] is the provision of the Service to its Clients. There is no other purpose for the collation, organisation and analysis of the data in this case other than the use of that data by the clients using the Service" ([141 of the FTT's decision); and

b. the potential subsequent use of profiling techniques by its clients.

314. There is also force in Mr Susskind's third reason for attacking the FTT's conclusion. The FTT's reasoning in [129] focuses in terms on the creation of the facial vectors (from the images scraped from the internet) and the indexing of the images it holds according to these facial vectors, whereas Clearview's processing of personal data extended significantly beyond this, as is apparent from the FTT's own findings as to the nature and extent of Clearview's processing, see [112] of the FFT's findings in particular. In assessing whether Clearview undertakes behavioural monitoring, we can see no good reason for confining consideration to the activities that the FTT addressed at [129].

315. In relation to the fourth alleged error, for the reasons set out in [256] to [275] and in [314] above, we find that Clearview's gathering, sorting and storing in a filing system organised person-by-person of "behaviourally rich" data (see the findings of fact set out in the FTT's decision at [22] to [69], and in particular at [38] and [49]) about natural persons amounts to "behavioural monitoring", properly construed.

316. There was evidence before the FTT that entitled it to conclude, as it did, that the data gathered by Clearview was "behaviourally rich". By way of example, in his cross-examination of Mr Mulcaire on day 1 of the FTT hearing (transcript at pages 59-60), Mr Pitt Payne put to Mr Mulcaire that Clearview had collected, sorted and stored the data relating to a specific individual shown at pages 1570 to 1662 of the FTT bundle.

317. The information Clearview had obtained, sorted and stored about this individual, highlighted features about him and about his behaviours. It included the individual having been:

a. photographed over time with the same child, permitting an inference that this individual might be a father (page 1604);

b. shown with a possible female partner (page 1628);

c. located at some point in Memphis, USA (text on page 1579);

d. shown smoking and gesturing with his middle finger to the photographer (page 1606);

e. shown drinking alcohol (page 1635);

f. shown performing musically at a specific time and place (page 1576);

g. shown performing a specific song that could be searched for elsewhere such as on streaming platforms (page 1612);

h. shown to have used social media (page 1579),

i. shown holding a large quantity of dollar bills (page 1589);

j. shown sitting in the driver's seat of a US car (page 1661);

k. shown with a handgun tucked into his belt or pocket (pages 1652 and 1658);

l. the subject of a police mugshot more than once (pages 1578 and 1584).

318. The information described above reflects the categories identified by the FTT at paragraph [49] of its decision. This information was already gathered and sorted by Clearview and was ready to be searched as a result of Clearview's Activity 1 processing even before any probe image of that individual might be uploaded by a Clearview client.

319. In relation to Mr Susskind's fifth point, Ms Proops submitted that, because of the way its system is engineered, Clearview has no ability to "see" the data it gathers and she argued that "watchfulness" was an important element of monitoring. However, the FTT did not use any of the anthropomorphised terms to which Mr Susskind objected in its explanation of its decision making on the issue of whether Clearview's processing involved behavioural monitoring. As such, we are not persuaded by this criticism.

320. Stepping back to assess Ground 3 in the round, we are persuaded that the FTT based its finding that Clearview does not itself undertake monitoring of UK data subjects within the meaning of Article 3(2)(b) GDPR on a misunderstanding of the proper meaning of "behavioural monitoring" for the purposes of Article 3(2) and an unduly narrow consideration of Clearview's processing activities. Had it applied the proper construction of "behavioural monitoring" (explained in [256] to [275] above) to the facts it found about Clearview's processing and about its clients' potential subsequent processing, the FTT would have been bound to find that Clearview's processing involved behavioural monitoring. We therefore find it made a material error of law.

Ground 4

321. Ground 4 argues that the FTT erred in failing to consider whether the ICO had jurisdiction in relation to Clearview's activities during the UK Test Phase. Mr Susskind pointed out that, contrary to what the FTT said, the MPN relied on the UK Test Phase, and he said the ICO never abandoned the claim to jurisdiction on that basis in the proceedings before the FTT. He took us to the transcript of Mr Pitt-Payne's cross-examination of Mr Mulcaire in the FTT proceedings, which did indeed refer to the UK Test Phase.

322. However, we note that the ICO did not pursue the case on jurisdiction arising from the UK Test Phase in any of the submissions that he made before the FTT. The ICO did not refer to this issue at all in his Re-Amended Response to Clearview's Statement of Facts and Grounds. That document runs to 77 pages and appears to provide a comprehensive response to Clearview's appeal grounds, including 25 pages dealing with issues relating to jurisdiction. Nor was it addressed in Mr Pitt-Payne's skeleton argument for the hearing before the FTT or in his oral submissions to the FTT.

323. In these circumstances and given the breadth and complexity of the contentions that were expressly ventilated below, although the point was not formally abandoned, we do not consider that the FTT's failure to appreciate

that the ICO still relied on the UK Test Phase, or to exercise its inquisitorial jurisdiction to consider the issue, can amount to an error of law. We therefore dismiss Ground 4.

Clearview's Additional Reasons

324. Clearview argued that the FTT erred in its decision making in relation to territorial scope, and proposed four "Additional Reasons" in favour of the conclusion that the ICO lacked jurisdiction.

Additional Reason 1

325. Clearview's Additional Reason 1 raises the issue whether Article 3(2)(b) can apply to the processing of a person where that person carries out no behavioural monitoring but their processing is "related to" behavioural monitoring carried out by another person.

326. Additional Reason 1 can only assist Clearview if we are wrong to have allowed Ground 3 (i.e. we are wrong to have found that Clearview itself engaged in behavioural monitoring).

327. We have already explained our construction of Article 3(2)(b) in [242] to [255] above.

328. The FTT gave the words "related to" as they apply to Article 3(2)(b) an expansive meaning, deciding that "nothing within [the GDPR] prevents the processing of data by a controller being "related to" the monitoring of behaviour by another distinct controller" (see [138] of the FTT decision).

329. The FTT's reasoning at [138] of its decision indicates that it was under a misapprehension about the facts of ***Soriano*** (wrongly believing it to have concerned separate parties conducting the processing and the monitoring). Further, we are not persuaded by the FTT's reasoning that if Clearview's narrow interpretation of "related to" were to apply, it would be easy for a party to circumvent Article 3 by delegating its processing and monitoring activities to separate persons to avoid coming within the scope of regulation, because such circumstances would give rise to an agency relationship.

330. However, while we do not agree with all of the FTT's reasons for its conclusion at [138] of its decision, we agree with its identification of the "mischief" at which the provision was targeted: it is "*the monitoring*", rather than who is doing the monitoring (reflected in the reference to "*the* monitoring" rather than "*their* monitoring" in both Recital 24 and in Article 3(2)(b) itself). We agree with the FTT's conclusion that Article 3(2)(b) applies to processing by one party which itself carries out no behavioural monitoring, provided that its processing is related to behavioural monitoring carried out by another party. We confirm the FTT's conclusion, albeit for the different reasons explained more fully at [242] to [255] above and we therefore dismiss Additional Reason 1.

Additional Reason 2

331. Clearview's Additional Reason 2 raises the issue whether Article 3(2)(b) can apply to processing by a controller on the grounds that such processing is

"related to" behavioural monitoring carried out by another party where that other party's behavioural monitoring is itself outside the scope of the GDPR.

332. Success on this ground can only assist Clearview if we are wrong to allow the ICO's Ground 3 (i.e. if we are wrong to conclude that Clearview's processing itself amounts to "behavioural monitoring").

333. Further, it can only assist Clearview in relation to its processing for its private sector contractor clients if we are also wrong to allow Ground 1 (i.e. if we are wrong to conclude that the FTT materially erred in finding that Clearview's contractor clients are beyond the material scope of the GDPR whether under Article 2(2)(a) or by independent operation of public international law).

334. While it is apparent from the pleadings and the transcript of the proceedings below that Clearview argued this issue before the FTT, unfortunately the FTT's decision is entirely silent on it. We cannot know whether the FTT considered it and rejected it, or whether it simply failed to reach any decision on it.

335. Clearview's case was that, because the "mischief" in the legislators' crosshairs was behavioural monitoring, if the only behavioural monitoring taking place was itself beyond the material scope of the GDPR, that behavioural monitoring must be ignored when the application of Article 3(2)(b) is being considered. If Clearview did not conduct behavioural monitoring itself, and if its clients' behavioural monitoring was outside scope, there was no "hook" to bring Clearview's processing within the territorial scope of the GDPR under Article 3.

336. The ICO's case was that Clearview's approach requires words to be read into Article 3 that the legislators have not chosen to include. Mr Pitt-Payne argued that had the legislators intended to restrict the application of the GDPR in the way suggested by Clearview, they could and would have said in terms that the related behavioural monitoring must itself be within the material scope of the GDPR.

337. Ms Proops said that, on the contrary, when the GDPR is read as a whole, it is apparent that there is no intention to extend the reach of regulation to behavioural monitoring carried out by a party who is out of scope.

338. We were not directed to any authorities to support either party's case in this regard.

339. The "mischief" at which Article 3(2) is aimed is behavioural monitoring. Its focus is on processing related to behavioural monitoring of data subjects and on the location of the data subjects being monitored. It is not on whomever is conducting the behavioural monitoring. Jurisdiction under the GDPR operates in two stages: first one must ascertain whether the processing in question is within the material scope of the GDPR under Article 2. That establishes whether or not the processing is of a kind that is of interest to the regulatory regime. Once material scope has been determined, one moves to the second stage, which is to consider whether the processing falls within territorial scope under Article 3.

340. In analysing this issue it is important to keep in mind that the Notices in this case were issued to Clearview, not its clients, and we have explained in [186] to [194] and [216] to [219] above why neither Article 2(2)(a) nor the independent operation of international law by reason of comity considerations takes Clearview's processing outside the material scope of the GDPR. Additional Reason 2 is really the counterpart to Clearview's case resisting ICO's Ground 2 (which we rejected for the reasons set out in [299] to [301] above). Given that we have rejected Clearview's intersectional analysis of Clearview's processing, there is no reason in principle why Clearview's processing related to its clients' behavioural monitoring should be excluded from the scope of regulation.

341. Ms Proops described Mr Pitt-Payne's interpretation as involving a kind of "jurisdictional hokey-cokey", meaning processing excluded at the first (material scope) stage in Article 2 is brought back in at the second (territorial) scope stage under Article 3. We disagree with this characterisation because the interpretation of Article 3 favoured by the ICO does not bring processing by a foreign state (or any other party enjoying immunity in accordance with comity principles) within the scope of regulation at the second stage, having been excluded under the first stage. It goes out at the first stage, and it stays out, without proceeding to the second stage under Article 3 at all. We consider that a natural interpretation of the provisions requires that where processing comes within material scope under Article 2, the issue whether the jurisdiction of the GDPR applies, depends only on whether the processing comes within territorial scope. That is determined by applying the test in Article 3 on its own, and it is impermissible to reopen the issue of material scope at the second stage.

342. Mr Pitt-Payne suggested that if we agree with Clearview that any behavioural monitoring excluded from material scope under Article 2 must be ignored for the purposes of ascertaining whether processing satisfies the Article 3 test, this would lead to absurd results, as described at paragraph [303] above. Mr Pitt-Payne argued that, following Clearview's approach, any behavioural monitoring by Clearview's UK competent authority client would have to be deemed not to exist for the purposes of applying the test under Article 3(2)(b) to Clearview, so Clearview's processing could not be brought within the territorial scope of the GDPR. In these circumstances, the processing by the client conducting the behavioural monitoring (that falls to be ignored for the purposes of Article 3(2)(b)) falls to be regulated under the Law Enforcement Directive and Part 3 of the DPA 2018. However, Clearview's processing on its behalf would be regulated under neither the GDPR, nor the Law Enforcement Directive nor the DPA 2018.

343. We are not persuaded by Clearview's proposed approach. While we have not found it necessary to determine whether this gives rise to absurdity, Mr Pitt-Payne's example of Clearview's processing related to the behavioural monitoring of a competent authority client demonstrates that it could give rise to surprising results.

344. Clearview's contended approach is not supported by the wording of Article 3. Furthermore, it is by no means necessary to infer from the words of Article 3

(or the GDPR read as a whole), any legislative intent to restrict the effect of Article 3(2)(b) by treating any processing falling outside scope under Article 2 as if it did not exist when considering whether either test in Article 3(2) is satisfied. Had that been the intention, it could have been written by the legislators into the Articles in a straightforward way, for example, by making Article 3 subject to Article 2. Neither is there anything to support it in the Recitals, the EDPB Guidelines or the Travaux. For these reasons, we dismiss Additional Reason 2.

Additional Reason 3

345. Clearview's Additional Reason 3 raises the issue whether Clearview's clients monitor the behaviour of UK data subjects, and whether Clearview's processing is "related to" this.

346. Clearview contends that, even if we reject its case on Additional Reason 1 (as we do) and we find that Article 3(2)(b) can apply where processing is carried out by one party and behavioural monitoring by another, we should find that the FTT erred in concluding that Article 3(2)(b) applied to the facts of this case.

347. Ms Proops argued that if Clearview's processing is treated as "related to" its clients' behavioural monitoring, this imposes an unfair burden on Clearview and on foreign controllers generally because a foreign controller cannot be expected to know what its clients do, and cannot be expected to know whether its clients are engaged in behavioural monitoring at all, which raises the important issue of legal certainty.

348. We did not find this argument persuasive. The FTT made extensive findings of fact about the way the Service operates and what the search results may be used for, including findings in relation to specific successful searches of the Clearview database that had been provided to Clearview by its clients (see [49] of the FTT's decision). We are satisfied there was evidence before the FTT allowing it to make those factual findings (see [316] to [318] above).

349. Clearview had also adduced considerable evidence before the FTT in the form of the "Lunch and Learn" materials which make clear that Clearview was selling its Service to clients on the basis of its potential as a tool for behavioural monitoring, and not simply as an identification tool. Those materials demonstrate that, while Clearview may not know in any particular case specifically what actions its clients actually take following receipt of search results, it is aware as a general matter of the nature of the use it is being put to, because that is the basis on which it has sold the Service: it is sold as a sophisticated tool designed to assist them with their investigations into national security and/or criminal law enforcement matters.

350. Ms Proops encouraged us to focus on processing only up until the production of the search results to the client, and not beyond, on the basis that the clients' subsequent activities were "too remote" or "not sufficiently closely connected". We can see no justification for such a limited approach, which is artificial and unsupported by authority. Given what Recital 24 and the EDPB Guidelines say, the FTT was clearly entitled to look beyond the Activity 2 processing and to take into account potential subsequent use of the data by Clearview's clients when assessing whether behavioural monitoring was being conducted.

351. Ms Proops argued that the words "related to" must be construed on the basis that there must be "the strongest possible connection" between Clearview's processing and the offending behavioural monitoring. We do not accept that there is any such requirement; it is not reflected in the expansive legislative wording or in any of the other materials that we were taken to. In any event, the FTT found that there was "such a close connection between the creation, maintenance and operation of the Database and the monitoring of behaviour undertaken by the clients that [Clearview]'s processing activities are related to that monitoring" (see [143] and [144] of the FTT's decision). These were findings the FTT was entitled to make.

352. We are satisfied the FTT was entitled to find that Clearview's clients engaged in behavioural monitoring and that Clearview's processing was "related to" the various forms that its clients' behavioural monitoring took, for the reasons the FTT gave at [117] to [121], [123] and [126] to [128] of its decision. We therefore dismiss Clearview's case on Additional Reason 3.

Additional Reason 4

353. Clearview's Additional Reason 4 raises the issue whether there was evidence before the FTT that was adequate to support its finding that its clients' behavioural monitoring was related to the personal data of data subjects in the UK in relation to their behaviour in the UK.

354. Success on this issue can only assist Clearview if we are wrong that Clearview itself was engaged in behavioural monitoring.

355. The FTT proceeded from its primary findings about the way that Clearview goes about scraping the public facing internet for data and the sheer size of its database (see its finding at [40] that it contains billions of images), to make a secondary finding by inference that it was "inevitable" that the database includes images of data subjects in the UK (see its finding at [131]). That was clearly a finding that was open to it, even in the absence of specific evidence of specific individuals whose personal data was included in Clearview's database.

356. The FTT proceeded from this finding, and its primary findings about the way that searches of Clearview's database are made, to infer that it was also "inevitable" that the vectors assigned to UK data subjects' facial images (constituting their personal biometric data) in the database will be processed during a search of the database since the matching process involves a comparison of the probe image uploaded by a client to Clearview's system against its entire database (see [131] of its decision). That finding was also clearly open to it.

357. Clearview maintained, though, that there was insufficient evidence before the FTT to permit a finding that its clients actually received data of UK data subjects in any search results or that they engaged in behavioural monitoring in respect of UK data subjects.

358. The FTT's findings in this regard were somewhat tentatively expressed: it said that it was "less likely that an image of a UK data subject will be produced as a successful match/partial match where the clients are investigating alleged

crimes/threats within their jurisdiction (i.e. not in the UK), unless the UK data subject is an international criminal, has become involved in activity the subject of investigation, or the client is investigating a multinational threat" (see the FTT's decision at [131]).

359. Clearview's witness, Mr Mulcaire, spoke in his evidence in terms of possibilities only. Ms Proops encouraged us to read the FTT's "less likely" in [131] (and the repetition of this phrase in [140]) of its decision) as meaning the converse of "more likely", and as indicating that it was not satisfied of this matter to the civil standard of proof. That is not the only way to interpret what the FTT said. We are satisfied that, when read in context, the FTT was simply indicating that the likelihood of the data of a UK data subject being provided to a client in a search result was "less likely" than the "inevitability" of Clearview's database including images of data subjects in the UK and the vectors assigned to their facial images being processed during a search of the database. When one reads on to [140], the FTT then expresses its conclusion in more conventional terms: "On the basis of our factual findings and having applied the law we have concluded that there is, more likely than not, monitoring of the behaviour of UK data subjects in the UK as far as their behaviour takes place within the UK" (our emphasis added).

360. Reading the decision as a whole, we are not persuaded that the FTT misdirected itself in law as to the appropriate standard of proof. We infer from the FTT's conclusion that it was "more likely than not" that monitoring of the behaviour of UK data subjects occurred that, despite Mr Mulcaire's evidence being expressed in terms of mere possibilities, the FTT was satisfied on the basis of the evidence as a whole that there was a greater likelihood of UK data subjects' data being included in a search result. Given 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, the FTT was entitled to conclude as it did.

361. Ms Proops also relied upon the principle of proportionality (see [177] above), arguing that even if the FTT was entitled to find that monitoring of the behaviour of UK data subjects took place, as far as their behaviour takes place in the UK, it would be wholly disproportionate for Clearview to be brought within the weighty and onerous GDPR regime as a result of what would be *de minimis* processing in this regard.

362. While we acknowledge that proportionality is a relevant consideration in the context of assessing the regulatory action taken against Clearview, we accept Mr Susskind's submission that issues of proportionality cannot be relevant to the binary question of whether or not the ICO had jurisdiction over Clearview's activities at all. There is nothing in the wording of Article 3(2)(b) to suggest that a *de minimis* threshold applies to the application of its criteria and there is nothing in the Recitals, the EDPB Guidelines or in ***Soriano*** to support this suggestion. The appropriate juncture at which to consider proportionality is at the substantive stage, when enquiring whether a penalty should be imposed and, if so, what that penalty should be. Ms Proops' submission elides these logically separate issues in suggesting that if it would be disproportionate to issue a penalty, the ICO should have no jurisdiction at all.

363. For these reasons we also dismiss Additional Reason 4.

Conclusion

364. The appeal against the FTT's decision that the ICO lacked jurisdiction to issue the Notices is allowed. That decision was materially in error of law and we set it aside. On a proper construction of the GDPRs the ICO had jurisdiction to issue the Notices.

365. As we have found at [186] to [195] and [216] to [219] above, Clearview's processing is not outside the material scope of the GDPR, either by virtue of Article 2(2)(a) or by the application of private international law comity principles, and the FTT erred in concluding that it was.

366. We have also affirmed the FTT's conclusion that Clearview's processing is within the territorial scope of the GDPRs. We have reached the latter conclusion on two alternative bases. First, that the FTT erred in concluding that Clearview's own processing did not amount to "behavioural monitoring": see [256] to [275] and [315] to [320] above. Second, because the FTT was correct to find that Clearview's processing was "related to" behavioural monitoring undertaken by its clients within the meaning of Article 3(2)(b) GDPR, albeit that our reasoning differs from the FTT's reasons in a number of respects: see [242] to [255] and [328] to [330] above.

367. We therefore remit this matter to a new FTT for consideration of the substantive appeal in accordance with our Directions.

The Hon. Mrs Justice Heather Williams DBE
Chamber President

Judge Thomas Church
Judge of the Upper Tribunal

Judge Judith Butler
Judge of the Upper Tribunal

Authorised for issue on 06 October 2025