Neutral citation number: [2023] UKFTT 00819 (GRC)

Case Reference: EA/2022/0165/FP

First-tier Tribunal
General Regulatory Chamber
Information Rights

Heard at: Field House, Breams Buildings, London

Heard: 21 to 23 November 2022
Decision given on: 17th October 2023

Before

TRIBUNAL JUDGE LYNN GRIFFIN
TRIBUNAL MEMBER STEPHEN SHAW
TRIBUNAL MEMBER ROSALIND TATAM

Between

Clearview AI Inc

Appellant

and

The Information Commissioner

Respondent

Representation:
For the Appellant: Anya Proops KC, Christopher Knight and Raphael Hogarth of counsel instructed by Jenner & Block London LLP
For the Respondent: Timothy Pitt-Payne KC and Jamie Susskind of counsel

Decision: The appeal is Allowed.

REASONS

1. We have concluded that the Information Commissioner ("the Commissioner") did not have jurisdiction to issue the Enforcement Notice and the Monetary Penalty Notice to Clearview AI Inc (referred to herein as "CV") because although the processing undertaken by CV was related to the monitoring of data subjects' behaviour in the United Kingdom, the processing is beyond the material scope of the GDPR and is not relevant processing for the purposes of Article 3 UK GDPR.

2. We find that the notices against which the appeal is brought were not in accordance with the law. Thus, the appeal is allowed.

The Enforcement Notice and the Monetary Penalty Notice

3. On 18 May 2022 the Commissioner issued two notices addressed to CV, an Enforcement Notice ("EN") and a Monetary Penalty Notice ("MPN"). These notices were predicated on the following propositions:

    a. CV is a controller of data as variously defined in sections 3(6) and 5 of the Data Protection Act 2018 ("DPA 2018"), Article 4(7) of the General Data Protection Regulation ("the GDPR"), and Article 4(7) of the UK General Data Protection Regulation ("the UK GDPR").

    b. CV's processing of the personal data of UK residents comes within (and/or has previously come within) the scope of the GDPR (in relation to processing taking place before 11PM on 31 December 2020); and the UK GDPR (in relation to subsequent processing), by virtue of Article 3(2)(b) GDPR and Article 3(2)(b) UK GDPR.

4. The notices alleged infringements of parts of Article 5 and Articles 6, 9, 14, 15-17, 21 & 22 as well as the duty to carry out a Data Protection Impact Assessment under Article 35 GDPR and UK GDPR.

5. Section 149 DPA 2018 gives a discretion to the Commissioner to issue an EN when the Commissioner is satisfied, inter alia, that the evidence demonstrates that a person has failed, or is failing to comply with the Articles relied upon by the Commissioner in this case, see section 149(2)(a)-(c).

6. The MPN was issued further to section 155 DPA 2018 which gives the Commissioner a power to impose a penalty in the form of an administrative fine as well as or in addition to any other measure taken, such as an EN, where the Commissioner is satisfied that there is a failure as outlined in section 149(2).

The Grounds of Appeal

7. By notice of appeal dated 29 June 2022 CV challenged not only the alleged breaches, asserting that there were none, but also the legality of the notices, disputing the characterisation of the Service offered by CV and disputing the jurisdiction of the Commissioner to issue notices to CV, averring that it is a foreign company providing its Service to "foreign clients, using foreign IP addresses, and in support of the public interest activities of foreign governments and government agencies, in particular in relation to their national security and criminal law enforcement functions", such functions being targeted at behaviour within their jurisdiction and outside of the UK.

8. The principal service offered by CV is provided to clients in support of the discharge of those clients' 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 CV. The Service is an internet search engine to which only the clients of CV have access. This is what we refer to in this decision as the Service.

The Issues for the determination of the preliminary issue

9. Whether or not CV has infringed the Articles of GDPR or UK GDPR as alleged or at all was not the issue before us. That would be the subject of any substantive hearing were this case to go forward.

10. The issues for us at this stage concern the jurisdictional challenge to the notices. We are invited by CV to allow the appeal, because the conditions provided for in Article 3(2)(b) of the GDPR &/or UK GDPR (i.e. the behavioural monitoring limb of Article 3) have not been met in respect of the Service. CV submits that the Commissioner was in error in deciding that the conditions were satisfied and that therefore the Commissioner was in error of law in deciding that the Service fell within the territorial scope of the GDPR and UK GDPR (together "the Regulations").

11. The argument under Article 3 was the focus of CV's submissions, however, CV also submits that were the criteria in Article 3(2)(b) to be met, both Article 2(2)(a) GDPR/ Article 3(2A) UK GDPR operate to take this case beyond the material scope of the Regulations.

12. The questions for us are whether:

    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, processing of data by CV was related to monitoring by either CV itself or by its customers;

    c. the processing by CV is beyond the material scope of the GDPR by operation of Article 2(2)(a) GDPR &/or is not relevant processing for the purposes of Article 3 UK GDPR thereby removing the processing from the material scope of UK GDPR.

13. CV's case is that the data processing undertaken by it in the context of the Service is outside the territorial scope of the Regulations, with the consequence that the ICO had no jurisdiction to issue the notices. CV further submits that the Service is an Internet Search Engine service which is offered exclusively to foreign (i.e. non-UK/EU) criminal law enforcement and national security agencies, and their contractors, in support of the discharge of their respective criminal law enforcement and national security functions which are

functions outside the material scope of the Regulations, pursuant to Article 2 of those Regulations.

14. In oral submissions it was accepted by the Commissioner that processing by a foreign government would not be within the scope of the Regulations due to the principles of international law that mean that one state cannot seek to bind another. The actions of a foreign state are out of scope, by application of Article 2(2)(a) GDPR and Article 3(2A) UK GDPR.

15. The allegations straddle the date on which UK GDPR came into force. There is no dispute that the effect in this case of the material terms of the substantive provisions are little different as between the GDPR and the UK GDPR, albeit that the route to the answer may be different.

16. It is also not disputed that the Commissioner has the power to issue an MPN in relation to contraventions of the GDPR which took place prior to 31 December 2020 by virtue of paragraph 2 of Schedule 21 to the DPA 2018, as inserted.

The Hearing

17. The hearing of the preliminary issue on jurisdiction took place at a face to face hearing. Having heard evidence and submissions we reserved our decision and met on more than one occasion to take our decision. I acknowledge and apologise for the time it has taken to reduce this decision to writing but this has been caused by not only the complexity and novelty of the issues but also a combination of circumstances including intervening judicial responsibilities.

The Evidence

18. No oral evidence was called on behalf of the Commissioner.

19. Thomas Mulcaire is General Counsel to CV. In his witness statement for the purposes of the preliminary issue hearing he said he was well versed in the Service provided by his employer and the technology that is behind it, but he has no qualifications in IT and is not a computer engineer. As his title suggests, Mr Mulcaire is a lawyer. Mr Mulcaire described the formation of the appellant company and the service provided by it as well as describing the activities undertaken by CV's clients from his own knowledge and from information provided to him by others. Mr Mulcaire was cross examined by Mr Pitt-Payne and asked questions by the Tribunal.

20. The core documents comprised 1662 pages, in the Updated Open Bundle. We also received a supplemental bundle of documents of 62 pages as well as bundles of authorities and skeleton arguments under separate cover. During the hearing we also received:

    a. Note of evidence heard on 21 November 2022 provided by the Commissioner,

b. Copy of the text of GDPR and UK GDPR Articles 2 and 3.

After the hearing we received CV's written reply to the oral submissions made on behalf of the Commissioner as there had been insufficient time to complete the appellant's reply at the hearing.

21. On the basis of all of the evidence, both oral and written, and having considered all the submissions made on paper, and at the hearing, about the weight that should be attached to the various types of evidence as well as to individual documents we have found the facts to be as follows.

The Facts

22. CV is incorporated in Delaware, in the United States of America and does not have and did not have (at the time of any of the alleged infringements) an establishment in the EU or UK as defined in the legislation.

23. In 2017 Mr Hoan Ton-That and Mr Richard Schwartz incorporated a company that was to become CV AI Inc upon a change of name in 2019. CV's principal place of business is New York City, but it operates remotely using a third-party computing platform to host its servers which are located in the state of Virginia. CV does not have any servers in the United Kingdom, nor does it use any IP addresses in the UK.

24. The Service is not currently used by clients in the UK nor in the EU; there was a UK trial phase - see below. CV has clients in the United States of America and in other countries around the world including Panama, Brazil, Mexico, and the Dominican Republic. Investigators in one country may be interested in behaviour happening in another country as criminal activity is not limited by national boundaries.

25. The Service is no longer offered by CV to commercial clients (that is to clients who would use the Service for commercial purposes) but prior to 2020 commercial clients were using the Service. This ceased as a result of the terms of a settlement agreed between CV and the American Civil Liberties Union, further details of which are given below, where this settlement is referred to as "the Illinois Settlement". During the period covered by the notices CV did not provide the Service to commercial clients.

26. We accept the unchallenged evidence of Mr Mulcaire that:

    a. All of CV's clients carry out criminal law enforcement and/or national security functions, and use the Service in furtherance of those functions.

    b. CV does not provide the Service to any clients outside the criminal law enforcement/national security context.

c. A decision was taken in May 2020 by CV to deactivate any remaining users that were not affiliated with government agencies or government agency contractors using the Service in support of their criminal law enforcement and national security functions.

d. CV's Terms of Service state, "Users shall only use the Services for legitimate law enforcement and investigative purposes", and "all Users are prohibited from engaging in the following acts: (i) using the Services for a commercial purpose" (Clauses 3.1.1 and 3.2.2 of the December 2021 version).

27. Delivering the Service entails the use of a database compiled by CV that is made up of interconnected sub-databases. The databases are separate but the images and related stored data in each independent database are connected by a unique identifier called a "blob ID". We will refer to the collection of sub-databases as the Database. The Database contains facial images in photographs which CV has copied/scraped from the public internet. We will call these the Stored Images.

28. The creation of the Database is, as described by the witness, 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 CV'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;

[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 CV 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.

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 CV employees.

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 CV open web scraper collects the most images, the website-specific scrapers are not deployed at all times.

30. CV 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 CV's clients.

32. Websites may contain instructions within them that instruct web crawlers not to access them, such as robot.txt files. CV'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 CV are not programmed to do this. So, if a page is password protected, CV's scrapers (both in-house and external) will not be able to access that page.

34. CV 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 CV for the Service. This protection relied on positive action being taken by the member of the public.

35. CV'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.

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

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 CV's scrapers copy only the image and additional information, not the entire page.

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". CV'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. CV'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. CV 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. CV 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 CV after what was referred to as the "Illinois Settlement" of 4 May 2022 in which CV 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. CV'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 CV 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 CV's clients wishes to use the Service, they will upload a facial image of an individual to CV'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, CV'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.

47. There are some analysis functions provided within the Service beyond the matching of the images. The system has a compare button which allows the client to view the Probe Image and the image returned by the search side by side and an image enhancement tool will upgrade and lighten low resolution images to improve the effectiveness of the search. The PDF export tool allows a client to share results within their agency and there is also an

ability to generate statistics about how the client is using the Service for the client's internal reporting or to account externally.

48. A client may use the results of the search to assist in making an identification or to assess what the person is doing when the photograph was taken from objects or activity shown within the image(s). Conclusions or inferences may be drawn from one, or more than one, image provided to the client as the results of their search, or from further information discovered by the client following the links provided with the search results. However, any such conclusions or inferences are made solely by the client and not by CV or its system. For example, the search may return numerous photographs of an individual participating in a sport from which a client may conclude that the person does so regularly, or is proud of so doing, as they frequently post pictures of themselves engaged in the activity. However, those would be deductions made by the human client who is viewing the results of the search.

49. Each CV client has an administrator that liaises with the client and can access details of the search history, but CV does not have access to the results of the searches, even though these are retained on its infrastructure, this is as a matter of choice built into the system. CV has been provided with some examples of successful searches by clients. Examples of the results of searches that we were provided with demonstrate that information and inferences may be drawn (from the images returned by the search coupled with the additional information and visiting the sources of the images) about:

   a. The person's name;

   b. The person's relationship status, whether they have a partner and who that may be;

   c. Whether the person is a parent;

   d. The person's associates;

   e. The place the photo was taken;

   f. Where the person is based/lives/is currently located;

   g. What social media is used by the person;

   h. Whether the person smokes/drinks alcohol;

   i. The person's occupation or pastime(s);

   j. Whether the person can drive a car;

   k. What the person is carrying/doing and whether that is legal;

l. Whether the person has been arrested.

50. These pieces of information are gleaned by deduction from the image or images returned by the search coupled with the additional information and also may require visiting the sources of the image(s). It would be unlikely for a single image to reveal all of the above. Such information may alternatively be discovered by way of a manual internet search, but this would be more time consuming and would depend on the effective construction of the search terms.

51. The search results may assist in the client making an identification of the person in the Probe Image, but it is for the client to make their own assessment using the results of the search in combination with other evidence they have gathered or will gather to establish the identity of the person. The search results may be the starting point for investigative steps that might not otherwise have been undertaken and may well be of importance to the eventual identification of the person in the Probe Image. The Service does not provide a definitive answer to the question of the identity of that person.

52. CV's terms and conditions reflected in the CV AI Code of Conduct, state "Search results established through CV and its related systems and technologies are indicative not definitive […] Law enforcement professionals must conduct further research in order to verify identifying information or other data discovered on third party sites by any CV system or included in CV search results. CV is neither designed nor intended to be used as a single-source system for establishing the identity of an individual". This means that CV requires its clients to use other investigative techniques to verify an identity before taking any action.

53. The Service will enable a client to "go beyond" the normal governmental databases as the CV Database will include images of people who have not come to the attention of the authorities in such a way as to result in an image of them being on the authorities' databases. The Service allows images from the internet to be used more effectively and efficiently by CV's clients by providing those leads more swiftly than a manual internet search using a traditional internet search engine would accomplish.

54. In theory a client could search against the same Probe Image on successive occasions, but the search results would reflect only those images that had been scraped by CV and would not necessarily represent an accurate reflection of the person's developing internet presence. The size of the internet means that CV does not copy every image that is posted online, and it does not try to. There may also be a delay between an image being posted online and the CV scrapers reaching that site or in revisiting it.

55. Until June of 2022 CV operated sessions for clients or trial users called "Lunch and Learn" the purpose of which was to demonstrate the effective use of the Service. The material relating to these sessions demonstrates the capabilities of the technology used by CV and the uses to which the Service could be put by CV's clients but not necessarily how it was in fact used. Potential uses include searching the internet for a known person by uploading a Probe

Image of that known person to attempt to find out where they are or to discover more about their activities. We were provided with an example of how the Service was instrumental in locating a person who was wanted by the authorities and who posted details of their travel arrangements enabling their detention.

56. These lunch and learn sessions also covered different aspects of CV's offering to their clients such as the creation of custom databases of images that are not drawn from the internet called "gallery functionality" intended for such uses as access control. Clients can search a Probe Image against their own gallery and the Database or could create a "most wanted list" as a customised gallery which can be searched against, with a Probe Image, either alone or in combination with the Database. There is also an alert function whereby an alert can be provided to a client if the Database acquires an image that matches the Probe Image or an image from the gallery. However, as stated by Mr Mulcaire, few CV clients use the gallery functionality at all or in these ways.

57. The offering from CV which facilitates the creation of an independent gallery, for example for the purpose of controlling access to premises, is known as "Clearview Consent". Clearview Consent is separate to the Service.

58. CV does not use any mechanism to detect the location of the server hosting a website and so it cannot tell if the server is in the UK. Nor does CV take steps to identify and/or block the creation of facial vectors from images where the EXIF data indicates it was taken in the UK. The geolocation data within EXIF data is not used to purge images taken in the UK. No analysis has been carried out by CV to identify what proportion of images that contain geolocation data were taken in the UK.

59. We have concluded that it is a reasonable inference that there are images of UK residents held within the Database given its size and the extent of internet and social media usage within the UK as compared to other countries where internet usage is not so prevalent. There will also be images taken while in the UK by or of persons resident elsewhere. However a comparison of likelihood of inclusion of images taken in a country appearing within the Database will not only depend on the internet/social media usage within that country but also upon where the web crawlers have visited and whether the social media users in that country are more or less likely to have activated privacy settings beyond which CV's scrapers will not copy images. Images on the internet may show a person in their home country or abroad. It is therefore not possible to predict with precision how many images will be included within the Database that are of UK residents and/or taken within the UK. It is not necessary for us to quantify either the number of images on the Database as a whole or those of UK residents or those taken in the UK. We proceed, for the purposes of the preliminary issue on the basis of our conclusion that there will be some images on the Database of data subjects taken within the United Kingdom.

60. As the Database holds images of UK residents which are compared to the Probe Images, and may be provided to the client as part of the search results, the Service offered by CV could have an impact on UK residents even though it is not used by UK customers.

61. CV does not use any website-specific scrapers directed at websites with any particular connection to the UK. There is no functionality provided for in CV's technology that can determine the residence of an individual captured in an image and it cannot realistically perform that function in respect of the contents of the Database as a whole. However, there are ways in which CV could identify Stored Images that retain their EXIF data indicating the place in which they were taken on the ways outlined above.

62. CV offered its Service on a trial basis to law enforcement/government organisations within the UK between June 2019 and March 2020. There were 721 searches made in that trial phase. This "UK Test Phase" took place before the end of the transition period associated with the withdrawal of the United Kingdom from the European Union. There is no suggestion that the Service has been offered to customers established within the UK since that time.

63. The UK Test Phase is not relied upon by the Commissioner as part of the alleged infringements but as an indication that there are images of UK residents held within the CV Database. It is argued that unless such images were held on the Database there would have been no point in UK law enforcement using the service. However, we were not told the reason the trial ended, nor whether it was unsuccessful and if so, the reason why nor whether the trial was terminated by CV or the potential clients trialling the Service. The possible reasons include that the Database did not include sufficient images of UK residents to make it of use to UK law enforcement, but we simply do not know, and we do not speculate. The reason for the termination of the UK Test Phase is not relevant to our deliberations given it is not relied upon as a foundation for jurisdiction.

64. An overseas law enforcement agency could use the Service as part of an investigation into the alleged criminal activity of a UK resident. They may use the Service as part of their investigation into a person's conduct or associates. Such is the international dimension of contemporary investigations into cross border criminal activity[4] that investigators in one country may very well be interested in behaviour happening in another country.

The Powers of the Tribunal

65. A person who receives an EN or an MPN may appeal the notice(s) to the Tribunal in accordance with sections 162(1)(c) and (d) DPA 2018 respectively. Where the appeal concerns an MPN it may be against the issue of the Notice, and/or the amount of the penalty in an MPN, see section 162(3) DPA 2018.

[4] For example, drugs offences, human trafficking or serious sexual offences.

66. Pursuant to the relevant parts of section 163 DPA 2018 the Tribunal has the following powers on an appeal brought under section 162(1):

s.163 (2) The Tribunal may review any determination of fact on which the notice or decision against which the appeal is brought was based.
(3) If the Tribunal considers—
(a) that the notice or decision against which the appeal is brought is not in accordance with the law, or
(b) to the extent that the notice or decision involved an exercise of discretion by the Commissioner, that the Commissioner ought to have exercised the discretion differently, the Tribunal must allow the appeal or substitute another notice or decision which the Commissioner could have given or made.
(4) Otherwise, the Tribunal must dismiss the appeal.

67. It is CV's case that the notices were not "in accordance with the law" because the Commissioner lacked jurisdiction, and that if the Tribunal agrees, we "must allow the appeal" it being inappropriate in those circumstances to substitute any notice(s).

68. The effect of allowing the appeal on those grounds would be to quash the notices albeit there is no explicit power to make such a quashing order within the legislation.

69. This is a decision on a preliminary issue within the context of a full merits review. As to the burden and standard of proof we respectfully agree with the decision of Judge Macmillan (as she then was) in the case of Doorstep Dispensaree Ltd v Information Commissioner (EA/2020/0065/V) in the context of MPNs[5]. The standard of proof to be applied in this case is the civil one. Our approach is to consider for ourselves whether or not the statutory criteria are met in the light of all the evidence and thereafter determine the consequences of those findings.

The Legal Framework

70. On 25 May 2018, the GDPR came into effect and was thereafter binding on the UK. On 26 June 2018 (after the decision to leave the EU) the UK enacted the European Union (Withdrawal) Act 2018, which retained the GDPR (with some amendments) as domestic law.

71. Thus an amended version of the GDPR would continue to apply in the UK following the completion of the Brexit implementation period on 31 December 2020 (IP completion day); this was named the UK GDPR. However, the UK GDPR is not a consolidated document. It is defined in section 3(10) of DPA 2018, supplemented by section 205(4). These provisions provide for the continued application of the GDPR subject to the amendments and interpretation principles set out in the DPA 2018.

[5] We note that the appeal against Judge Macmillan's decision has since been dismissed by the Upper Tribunal, see [2023 UKUT 132 (AAC)

72. Both the GDPR and UK GDPR have some extraterritorial scope by virtue of Article 3 of each regime and as regards the UK, section 207 of the DPA 2018. This decision is about the whether the extraterritorial scope extends to cover the activities of CV.

73. Article 3 GDPR states, as relevant to 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 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

74. As regards the territorial scope of the UK GDPR, Article 3 UK GDPR provides as follows:

(1) This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the 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.

75. The Commissioner issued the notices in this case on the basis that the Service falls within the territorial scope of the Regulations solely on the basis that it is caught by the terms of Article 3(2)(b) the substance of which has not changed between GDPR and UK GDPR.

76. There are four common elements in each version of the Regulation to be satisfied for the successful application of the criterion under Article 3(2)(b) bringing processing within the territorial scope of the regulation:

    a. There must be processing of personal data.

    b. The personal data must be that of data subjects in the UK.

    c. The processing must be carried out by a controller or processor not established in the UK.

    d. 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.

77. In so far as UK GDPR is concerned there is a fifth element; this is that the processing must be relevant processing as defined in Article 3(2A), see above text. Relevant processing does not include processing described in Article 2(1)(a) UK GDPR. We will return to this in relation to material scope.

78. Not all processing by a non-UK controller or processor is regulated; a controller or processor may be subject to the Regulation in respect of some of its processing activities but not others. For Article 3(2) to be engaged in either GDPR or UK GDPR, the processing must be "related to" one of the limbs triggering Article 3(2). The Commissioner relies on limb (b) in Article 3(2).

79. We were provided with a large number of authorities but only one that directly appertains to the construction of Article 3 (Soriano, see below). We have read the decisions of other regulators from around Europe but it is not suggested that these are binding upon us. They are placed before us by the Commissioner to demonstrate the level of concern that has arisen about the Service provided by CV but that is not a relevant consideration. We also note that those regulators have taken regulatory steps because they received complaints from data subjects within their jurisdiction. There is no evidence of such complaint in this case placed before us by the Commissioner; albeit there is reference in representations made on behalf of CV to two complaints being raised with CV by the Commissioner. However, the Commissioner as regulator, did not begin the investigation on the basis of any such complaints in this case. Those decisions of the First Tier Tribunal that have been referred to are not binding upon us.

80. In Soriano v Forensic News LLC and others [2021] EWCA Civ 1952 the Court of Appeal considered whether the publication of personal data of an individual in the EU by a

publication based in the United States of America could be related to the offering of goods or services or monitoring behaviour in the EU (Article 3(2)(a)). The Court of Appeal held that:

a. It was "arguable" that journalistic processing could be related to an offer made by a controller to data subjects in the EU to provide them with services in the form of journalistic output, and that this could fall within the meaning of Article 3(2)(a) of the EU GDPR.

b. There was a "compelling case" on the facts of Soriano that:

   i. preparatory activities such as assembling, analysing and ordering information about the behaviour of an individual in the EU would be engaging in monitoring within the meaning of Article 3(2)(b); and

   ii. such preparatory activities are related to (in fact, integral to) the publication of personal data about the individual in question, which is a form of processing.

81. However, Soriano did not decide these issues conclusively because for the purposes of that appeal the claimant only had to show that he had a real, as opposed to a fanciful prospect, of success on the claim which he wanted to serve on a defendant outside of the UK. Therefore, these examples are not definitive examples of what processing might be related to the monitoring of the behaviour of data subjects in the UK as far as their behaviour takes place within the UK. However, as observations made by the Court of Appeal we acknowledge their persuasive weight.

82. Recital 24 of the GDPR is relevant to the construction of Article 3(2)(b) GDPR and Article 3(2)(b) UK GDPR, this reads as follows:

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.

83. Guidance issued by the European Data Protection Board (EDPB) as to the application of GDPR provides an indication of how Article 3(2)(b) may be understood. This guidance indicates that although absent from the wording of Article 3(2)(b) or in the recitals to the GDPR, the language implies that an element of targeting and intentionality is required. The guidance from the EDPB suggests that the word "monitoring" implies that a controller has in

mind a specific purpose for the collection and reuse of the relevant data about an individual's behaviour within the EU. Thus and with reference to specific examples within their guidance the EDPB considers that not all online collection or analysis of personal data of individuals in the EU amounts to monitoring. The issue should be determined on a case by case basis; regard being had to the controller's purpose for processing the data and conducting behavioural analysis.

84. The EDPB Article 3 Guidelines also suggest that for limb (b) of Article 3(2) to be triggered, the monitored behaviour must take place within the territory of the EU (see page 19 of those guidelines).

85. As set out above Recital 24 provides guidance about the types of activities that are intended to be captured by this limb. The specific activities contemplated in Recital 24 are tracking on the internet, including profiling an individual, such as to make decisions in respect of them or predicting their personal preferences, behaviours and attitudes. However, the EDPB notes that the operation of Article 3(2)(b) is not limited to monitoring over the internet. Tracking through other types of networks or technology involving processing personal data (such as via wearable smart devices) may also be caught by this limb.

86. *Personal data* is "any information relating to an identified or identifiable living individual": see section 3(2), DPA 2018. The section also defines *"Identifiable living individual"* as meaning a living individual who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data or an online identifier, or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the individual.

87. The same section states that *"Processing"*, in relation to information, means[6] an operation or set of operations which is performed on information, or on sets of information, such as the following:

    a. collection, recording, organisation, structuring or storage,

    b. adaptation or alteration,

    c. retrieval, consultation or use,

    d. disclosure by transmission, dissemination or otherwise making available,

    e. alignment or combination, or

    f. restriction, erasure or destruction.

[6] subject to subsection (14)(c) and sections 5(7), 29(2) and 82(3),

88. Certain terms used in GDPR/UK GDPR are defined in the Regulation(s) but others are not, relevant definitions within Article 4 include:

4(1) 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

4(2) 'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

4(4)'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, health, personal preferences, interests, reliability, behaviour, location or movements;

4(7)'controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; [the following text is added in GDPR that does not appear in UK GDPR - where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law];

4(14)'biometric data' means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data;

89. Article 2 of the GDPR/UK GDPR is headed "Material scope". The text has changed but the substance of the relevant question for us is the same.

90. Article 2(2) of the GDPR provides as follows, it will be noted that the text excludes specified types of processing from the application of the Regulation:

2(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."

91. The relevant paragraph in Article 2(2) GDPR is 2(2)(a) in relation to which Recital (16) provides:

"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."

92. Recital (19) provides, insofar as relevant:

"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."

93. Conversely Article 2 of the UK GDPR provides in full as follows, it will be noted that there is no provision disapplying the Regulation such as Article 2(2)(a) of the GDPR. In fact the activities specified within that part of the GDPR are placed within the scope of UK GDPR by Article 2(1)(a) UK GDPR:

2(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.

4. This Regulation shall be without prejudice to the application of the Electronic Commerce (EC Directive) Regulations 2002, in particular the provisions about mere conduits, caching and hosting (see regulations 17 to 19 of those Regulations).

5. In this Article—

(a) 'the automated or structured processing of personal data' means—

(i) the processing of personal data wholly or partly by automated means, and

(ii) the processing otherwise than by automated means of personal data which forms part of a filing system or is intended to form part of a filing system;

(b) 'the manual unstructured processing of personal data' means the processing of personal data which is not the automated or structured processing of personal data;

(c) 'FOI public authority' has the same meaning as in Chapter 3 of Part 2 of the 2018 Act (see section 21(5) of that Act);

(d) references to personal data 'held' by an FOI public authority are to be interpreted in accordance with section 21(6) and (7) of the 2018 Act;

(e) 'competent authority' and 'law enforcement purposes' have the same meaning as in Part 3 of the 2018 Act (see sections 30 and 31 of that Act).

94. There is a specific directive that applies to the activities of law enforcement agencies, that is the Law Enforcement Directive. That directive regulates the processing of data in relation to law enforcement purposes which are 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. However, its application was not in issue before us nor was the issue of whether CV or its client may be regarded as a competent authority.

95. We indicated earlier that we would return to Article 3(2A) UK GDPR which reads:

3(*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).*

96. Article 2(1)(a) UK GDPR explicitly applies the Regulation to automated or structured processing[7] in the course of an activity which, immediately before IP completion day, fell

[7] It was not in dispute that the processing with which we are concerned was automated/structured.

outside the scope of EU law. However, where all the other elements of Article 3 UK GDPR are satisfied, Article 3(2A) operates to remove the CV processing from the scope of the Regulation because it is not within the definition of "relevant processing" as required by Article 3(2).

97. Thus, although the legislative route has changed the question remains the same –

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

We have concluded that if the answer is yes then either

a. GDPR Article 2(2)(a) disapplies the Regulation, taking the processing beyond the material scope of the Regulation (GDPR), or

b. In UK GDPR by application of the definition of "relevant processing" in Article 3(2A), the fifth element (as we have called it in paragraph 77) within Article 3(2) UK GDPR will not be satisfied and the processing will be beyond the scope of the Regulation (UK GDPR).

The Commissioner's case in the notices

98. The Commissioner submits that there are two types of activity as reflected in the notices:

a. Activity 1 processing, covering the creation, development and maintenance of the Database;

b. Activity 2 processing, namely CV'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.

99. It is said that CV is the sole controller responsible for Activity 1 processing but shares that role with its client so far as Activity 2 processing is concerned.

100. The Commissioner's case is that it is CV's clients who are monitoring the behaviour of UK residents and thus the processing carried out by CV as sole or joint controller is "related to" the monitoring of behaviour of UK residents.

101. The monitoring of behaviour that is relied upon is that CV's clients "may be able to ascertain information about a particular individual's behaviour, not only at a particular point in time, but extending over a period of time".

102. The Commissioner states that CV will be responsible for processing by its clients because of the "very close relationship" between CV's activities and those of its clients who are conducting the behavioural monitoring.

103. It is said that those individuals who are being "monitored" will inevitably, by inference, include UK residents given the size and source of the database.

104. It became clear that there was some dispute about the extent of reliance upon two aspects of the case, first the "Indexing case" and secondly the "Future use" case.

105. The indexing case is not clearly relied upon in the EN/MPN; it is implied rather than explicit. That may be because its significance was not recognised at the time. The term indexing refers to the organisation of the facial vectors created as a means of facilitating the search thereby providing greater efficiency and speed. It is a mathematical process that does not change the fundamentals of the processing of the data. It seems to us that indexing is an integral part of the function of the Service falling under the category of Activity 1 processing which increases the efficiency of Activity 2 processing. This is the secondary case for the Commissioner in that this is the basis on which it is asserted that CV is monitoring behaviour itself.

106. As to any future use of the Service, this is irrelevant to the issue of whether the Commissioner has jurisdiction to issue the notices in this case. The Commissioner suggested that because CV may offer the service beyond the law enforcement community, at some future unspecified date, this affects whether the current processing is within the scope of the Regulations. However, the evidence does not reflect such an intention and we have concluded that approach would be speculative.

107. Subsequent to the ruling of Judge Griffin (dated 15 November 2022) on the issue of disclosure the Commissioner withdrew reliance on the potential future commercial use of the Service.

CV's case in response to the notices

108. CV submits (in summary) that the notices are founded on fundamental errors of law and fact. This is because:

a. the data processing undertaken by CV in the context of the Service is outside the territorial scope of the Regulation, with the consequence that the ICO had no jurisdiction to issue the notices;

b. the notices are fatally flawed by both unsustainable findings of breach and a wrongful exercise of discretion, this is the substantive challenge made subject to the resolution of the jurisdiction issue above.

109. As to the issue of jurisdiction CV submits that:

a. It is clear from the terms of the notices which mirror the content of the notice of intent and preliminary enforcement notice, that the MPN and EN are both exclusively concerned with CV's data processing in the context of the Service (see EN §§39-44 and MPN §§44-49).

b. Article 3(2)(b) does not apply. The Service is a technology support service, supporting third party activities that are themselves entirely outside the material scope of the Regulations by enhancing the ability of the clients to search for and locate facial images of criminal suspects and suspected victims of crime which have been published to the world at large on the public internet, with a view to the clients using those images (i.e., the relevant search results) within their wider investigative activities so as to identify those suspected criminals and victims of crime. The Service is not capable of recognising or analysing behaviours.

c. CV is not aware of their clients using the results provided by the Service in the context of behavioural monitoring. Any behavioural information would be revealed in an ad hoc fashion and has already been published to the world on the internet. It may not be relevant to the investigation and is likely to be only one source of information used in the course of the client's investigation. However, if the search results were being used in this way it does not detract from the primary value of the Service as a tool for swiftly identifying an individual.

d. The Service is an internet search engine service offered exclusively to foreign (i.e., non-UK/EU) criminal law enforcement and national security agencies, and their contractors, in support of the discharge of their respective criminal law enforcement and national security functions.

e. The Service itself is aimed at supporting CV's foreign (non-UK/EU) clients in discharging their foreign (non-UK/EU) criminal law and national security functions, which functions are predominantly domestically preoccupied. Such functions are outside the material scope of the Regulations, pursuant to Article 2 of those Regulations.

Conclusions and Reasons

110. Having found the facts as above we applied the law as set out in our description of the legal framework and conclude as follows. In doing so we are grateful for the detailed submissions of the parties which we have considered in taking our decisions even if they are not referenced specifically below.

111. We agree, and there was no dispute, that the images and additional information that are held in the CV 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. CV 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 CV 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 CV includes the following types of processing that would fall within the definition provided in Article 4(2):

a. upload of probe image to CV;

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 CV 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 CV 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. CV'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 CV'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 CV, 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 CV'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 CV 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 CV 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 CV Service as described above CV'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 CV Database, and/or by considering those search results in conjunction with the Probe Image, or other information gathered as part of their investigation, CV'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 CV 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 CV 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 CV'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 CV 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 CV'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. CV is a controller of the data as regards Activity 1 processing. This was not in dispute.

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

a. CV determines the purposes of the processing as it only provides the Service to those who wish to use it for purposes agreeable to CV within its terms and conditions, for example not for any other purpose than matters of law enforcement and national security;

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

137. CV 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 CV 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 CV 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 CV'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 CV 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. CV 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 CV's processing activities are related to that monitoring.

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

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

b. The purpose of CV's Activity 2 processing is to provide CV's image matching service to its clients, thereby enabling the monitoring of behaviour carried out by CV'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. CV 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 CV'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 CV 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 CV 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 CV 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 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 CV'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 CV'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 CV was related to the monitoring of behaviour by CV'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.

158. Therefore, it is our conclusion that the Commissioner did not have jurisdiction to issue the EN or MPN. The notices against which the appeal is brought were not in accordance with the law.

159. For all these reasons the appeal is allowed.

Coda

An embargoed copy of this decision was circulated to the parties. We are grateful to the parties for their careful attention to the draft and their suggested corrections and clarifications.

Signed: *Judge Lynn Griffin* Date: 17 October 2023