DATA PROTECTION ACT 2018
(PART 6, SECTION 149)

ENFORCEMENT POWERS OF THE INFORMATION COMMISSIONER

ENFORCEMENT NOTICE

To: Clearview AI Inc

Of: 99 Wall Street
#5730 New York
N.Y. 10005

1. Clearview AI Inc ("**Clearview**") is a "controller" 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").

2. Clearview's processing of certain personal data 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.

3. The Information Commissioner ("**the Commissioner**") hereby issues Clearview with an Enforcement Notice under section 149

DPA 2018. The Notice is in relation to Clearview's continuing infringements of:

(i) the data protection principles set out in Article 5(1)(a) and Article 5(1)(e) UK GDPR;

(ii) the requirements of Article 6 UK GDPR as to the lawful basis for the processing of personal data;

(iii) the requirements of Article 9 UK GDPR as to the processing of special category personal data;

(iv) the requirements of Article 14 UK GDPR as to the information that is to be provided by controllers to data subjects;

(v) the requirements of Articles 15, 16,17, 21 and 22 UK GDPR in relation to the rights of data subjects; and

(vi) the duty to carry out a Data Protection Impact Assessment under Article 35 UK GDPR.

This Notice is accordingly issued under section 149(2)(a), (b) and (c) DPA 2018.

4. This Enforcement Notice relates to Clearview's continuing infringements of the UK GDPR in the respects set out at paragraph 3 above. However, in order to explain the basis and context for the Commissioner's decision to impose an Enforcement Notice, it is necessary to refer also to various past infringements by Clearview of the GDPR and UK GDPR.

5. This Notice explains the Commissioner's decision to take enforcement action. The specific steps that Clearview is required to take are set out in Annex 1.

6. The Commissioner has previously served Clearview with a Preliminary Enforcement Notice ("the PEN") dated 23 November

2021. Clearview provided its written representations ("the Representations") in response to the PEN, on 3 February 2022. The Commissioner has taken into account the entirety of the Representations when deciding to issue this Notice and refers to the Representations below when appropriate.

Legal framework for this Notice

7. DPA 2018 contains various enforcement powers in Part 6 which are exercisable by the Commissioner.

8. Section 149 DPA 2018 materially provides:

> *(1) Where the Commissioner is satisfied that a person has failed, or is failing, as described in subsection (2), (3), (4) or (5), the Commissioner may give the person a written notice (an "enforcement notice") which requires the person—*
>
> *(a) to take steps specified in the notice, or*
>
> *(b) to refrain from taking steps specified in the notice,*
> *or both (and see also sections 150 and 151).*
>
> *(2) The first type of failure is where a controller or processor has failed, or is failing, to comply with any of the following—*
>
> *(a) a provision of Chapter II of the GDPR or Chapter 2 of Part 3 or Chapter 2 of Part 4 of this Act (principles of processing);*
>
> *(b) a provision of Articles 12 to 22 of the GDPR or Part 3 or 4 of this Act conferring rights on a data subject;*

(c) a provision of Articles 25 to 39 of the GDPR or section 64 or 65 of this Act (obligations of controllers and processors);

(d) a requirement to communicate a personal data breach to the Commissioner or a data subject under section 67, 68 or 108 of this Act;

(e) the principles for transfers of personal data to third countries, non-Convention countries and international organisations in Articles 44 to 49 of the GDPR or in sections 73 to 78 or 109 of this Act.

(6) An enforcement notice given in reliance on subsection (2), (3) or (5) may only impose requirements which the Commissioner considers appropriate for the purpose of remedying the failure.

9. Section 150 DPA 2018 materially provides:

(1) An enforcement notice must—

(a) state what the person has failed or is failing to do, and

(b) give the Commissioner's reasons for reaching that opinion.

(2) In deciding whether to give an enforcement notice in reliance on section 149(2), the Commissioner must consider whether the failure has caused or is likely to cause any person damage or distress.

(3) In relation to an enforcement notice given in reliance on section 149(2), the Commissioner's power under section 149(1)(b) to require a person to refrain from taking specified steps includes power—

(a) to impose a ban relating to all processing of personal data, or
(b) to impose a ban relating only to a specified description of processing of personal data, including by specifying one or more of the following—

(i) a description of personal data;
(ii) the purpose or manner of the processing;
(iii) the time when the processing takes place.

(4) An enforcement notice may specify the time or times at which, or period or periods within which, a requirement imposed by the notice must be complied with (but see the restrictions in subsections (6) to (8)).

10. In relation to the application of the GDPR, Article 3 GDPR materially provides as follows:

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

(2) This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or

processor not established in the Union, where the processing activities are related to:

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

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

11. In relation to the application of the UK GDPR, Article 3 UK GDPR materially 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.

12. When construing Article 3(2)(b) GDPR and Article 3(2)(b) UK GDPR, recital 24 to the GDPR is relevant. 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.

13. The data protection principles are now set out in Article 5(1) UK GDPR. By Article 5(2), the controller shall be responsible for, and to be able to demonstrate compliance with, paragraph 5(1).

14. Paragraph 5(1) UK GDPR includes the following requirements:

(1) By paragraph 5(1)(a), that personal data are to be processed lawfully, fairly and in a transparent manner in relation to the data subject ("lawfulness, fairness and transparency");

(2) By paragraph 5(1)(e), that personal data are to be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed ("storage limitation").

15. Article 6 UK GDPR provides that processing of personal data shall be lawful only if and to the extent that one of the provisions in Article 6(1) applies.

16. Article 9(1) UK GDPR provides that processing of special category personal data (as defined in Article 9(1)) shall be prohibited. Article 9(2) disapplies Article 9(1) where one of the provisions in Article 9(1)(a)-(j) applies.

17. Chapter III of the UK GDPR makes provision for the rights afforded to data subjects. These include, by Articles 13 and 14, the right to receive from the controller certain information about the processing of their personal data. In the present case, Article 14 would be relevant, as it sets out the information to be provided where (as here) the controller has obtained personal data other than from the data subject.

18. Articles 15, 16, 17, 21 and 22 UK GDPR set out the rights of the data subject in relation to the following (respectively): right of access to personal data; rectification of personal data; erasure of personal data; objection to the processing of personal data; and automated processing.

19. Article 35 UK GDPR requires a controller to carry out a Data Protection Impact Assessment (DPIA) in specified circumstances.

20. In relation to the provisions of the UK GDPR referred to at paragraphs 13-19 above, there is no material difference between the GDPR and the UK GDPR.

Factual findings in relation to the service provided by Clearview

21. Clearview operates an algorithmic image search engine. It provides a service whereby a customer can seek to match an image that is of interest to the customer (a "Probe Image") against a database of images, metadata and URLs held by Clearview (the "Clearview Database").

22. The service provided by Clearview operates in the following way. The customer provides Clearview with a Probe Image. Clearview compares the Probe Image with the Clearview Database and provides its customer with an indexed list of images from the Clearview Database that have similar characteristics with the Probe Image: this list consists of a set of thumbnail search results, with a link in each case to the URL where the image appears online. So that it can compare the Probe Image with the images in the Clearview Database, Clearview derives a set of facial vectors from the Probe Image ("the Probe Vectors"); when a search of the Clearview Database is carried out, the Probe Vectors are compared against facial vectors drawn from the images in the Clearview Database ("the Database Vectors").

23. The customer's purpose in using the Clearview service is to be able to identify the individual who appears in the Probe Image, and/or to find out more about that individual. For instance, the Probe Image may be of a suspect in a criminal investigation, or may show

an individual taking part in what appears to be criminal activity. Clearview does not provide its customer with any opinions as to the identity, or attributes, of the individual shown in the Probe Image. Rather, Clearview provides a set of search results showing images from the Clearview Database that have similar characteristics to the Probe Image (as determined by comparing the Probe Vectors and the Database Vectors). Once the search results have been provided, it is for the customer to examine the URLs for those images. By doing so, the customer may discover information as to matters such as the identity, attributes, location, movements and behaviour of the individuals whose images are included in the Probe Image and/or in the search results.

24. The Commissioner understands that the images, metadata and URLs in the Clearview Database have been obtained (or "scraped") from the public-facing internet worldwide (including from social media websites).

25. Further, the Commissioner understands that Clearview takes no steps to exclude images of UK residents, or images showing their behaviour in the UK, from the Clearview Database.

26. Clearview's web page currently indicates that the Clearview Database holds over 10 billion images (having previously given a figure of 3 billion images). Recent media coverage has indicated that the database now holds some 20 billion images[1]. It is apparent from this material that the number of images on the Clearview Database has been increasing, and continues to

[1] See the recent interview with Clearview's co-founder featured on the BBC news website on 20 April 2022: https://www.bbc.co.uk/news/av/world-us-canada-61123510

increase. There is nothing in the Representations to suggest otherwise.

27. Clearview has not informed the Commissioner as to the number of images of UK residents that it holds. In an enquiry response to the Commissioner dated 21 July 2020 Clearview expressly stated that it was unable to provide the Commissioner with this information.

28. The Clearview service has previously been used on a trial basis by customers established in the UK (the Commissioner refers to this as "the UK Test Phase"). The Commissioner understands that at least 5 UK law enforcement organisations used the service during the UK Test Phase, and that some of them returned matches for individuals of interest to them. The Commissioner also understands that a total of about 721 searches using Probe Images were carried out by 5 different UK law enforcement agencies during the UK Test Phase. Some of these were duplicate searches (i.e. more than one search was carried out in respect of the same individual), but the total number of searches carried out gives some indication as to the number of UK individuals included in the searches.

29. The fact that the UK Test Phase was carried out at all, in itself indicates that the images of a very substantial number of UK residents must have been included on the Clearview Database at that time; otherwise, there would have been no point in Clearview carrying out the UK Test Phase, since there would have been little prospect that Probe Images submitted by UK law enforcement agencies would have matched any of the images on the Clearview Database. Further, in a number of cases the Clearview Database returned matches for Probe Images submitted during the UK Test

Phase; this likewise indicates that the images of a very substantial number of UK residents were at that time held on the UK database.

30. The UK Test Phase was completed before the end of the transition period associated with the withdrawal of the United Kingdom from the European Union. The Commissioner is satisfied on a balance of probabilities that Clearview is not currently offering services to customers established in the UK (whether in the law enforcement sector or otherwise). There is however no indication whatsoever that Clearview has taken any steps since the end of the UK Test Phase to reduce the number of images of UK residents that are held on the Clearview Database. There is no suggestion whatsoever in the Representations that Clearview has taken any such steps. On the contrary, it is apparent – from the figures referred to at paragraph 26 above – that the number of images held on the Clearview Database has continued to increase.

31. Even leaving aside the matters set out above in relation to UK Test Phase it is in any event inevitable that images of a very substantial number of UK residents (including images of their behaviour in the UK) will be included on the Clearview Database, given that: (a) the Clearview Database now includes 10 billion images, or more; (b) no steps are taken to exclude images of UK residents (or images of their behaviour in the UK) from the Clearview Database; and (c) there is extensive internet and social media usage within the UK. By way of illustration of point (c):

    - The Office for National Statistics (ONS) estimates that in early 2020 96% of households in Great Britain had internet access; and

- In its "Online Nation" report of 2020, OFCOM estimated that social media and messaging sites reached 98% of the UK adult digital population and that on average individuals aged 18 or over spent 49 minutes per person per day on social media sites.

32. Clearview continues to offer and provide its services to customers not established in the UK. It follows that Clearview: (a) continues to compare Probe Images of UK residents against the Clearview Database, when such Probe Images are submitted by its customers; and (b) continues to compare images of UK residents held in the Clearview Database, with Probe Images submitted by its customers. The operation of the Clearview service therefore continues to have a significant impact on UK residents, notwithstanding that Clearview does not currently offer its services to UK customers.

Clearview processes the personal data of substantial numbers of UK residents, and does so as a controller

Clearview processes the personal data of substantial numbers of UK residents

33. The images, metadata and URLs that are held in the Clearview Database constitute personal data. In particular: (a) an image of an identifiable individual, held in the Clearview Database, would constitute personal data about that individual; and (b) any metadata and URLs associated with such an image would likewise constitute personal data about the individual in question. Further, the Database Vectors derived from any such images would constitute special category data within the meaning of Article 9(1)

GDPR and UK GDPR (since the Database Vectors would constitute biometric data falling within Article 9(1)).

34. By obtaining images from the public facing internet, holding them on the Clearview Database, and generating the Database Vectors from them, Clearview processes personal data (including special category data).

35. Likewise, a Probe Image constitutes personal data about the individual shown in that image, and the Probe Vectors derived from the Probe Image would constitute special category data (as they are biometric data falling within Article 9(1)).

36. When Clearview seeks to match a Probe Image against the Clearview Database, Clearview thereby processes: (a) the personal data in the Probe Image (including the special category data consisting of the Probe Vectors); and (b) personal data in the Clearview Database (including the special category data consisting of the Database Vectors), i.e. the personal data contained in or associated with any images in the Clearview Database that are compared against or matched with the Probe Image.

37. Given the factual findings set out at paragraphs 21 – 32 above, Clearview's processing of personal data has included and continues to include the processing of the personal data of a very substantial number of UK residents.

38. The processing of such personal data about UK residents will inevitably include the processing of personal data about their behaviour in the UK.

- Images scraped from the public facing internet will include (or will in some cases be derived from) images

showing individuals engaged in specific activities (i.e. images that are disclosive of information about the individual's behaviour). There is no suggestion whatsoever that Clearview seeks to exclude images of this nature from the Clearview Database.

- Given the nature of the service provided by Clearview, and the purposes for which that service is used by Clearview's customers, Probe Images will inevitably include (or will in some cases be derived from) images that show individuals engaged in particular activities (i.e. images that are disclosive of information about the individual's behaviour).

- Images that are disclosive of information about a UK resident's behaviour are more likely than not to relate to their behaviour *in the UK* (since such individuals are likely to spend substantially more of their time in the UK than overseas).

Clearview processes personal data as a controller

39. The Commissioner considers that the processing of personal data by Clearview (as set out above) can be divided into two overarching types of processing: "Activity 1 Processing" and "Activity 2 Processing". For the reasons set out below, the Commissioner considers that Clearview is and at all material times has been: (a) sole controller in relation to Activity 1 Processing; and (b) a controller (along with its customer) in relation to Activity 2 Processing.

40. Activity 1 Processing consists of Clearview's creation, development and maintenance of the Clearview Database.

41. As set out above, Activity 1 Processing involves the processing by Clearview of personal data consisting of the images of identifiable individuals (and metadata and URLs associated with those images) together with Database Vectors derived from those images. Clearview processes such data both by obtaining it (that is, by scraping it from the public-facing internet) and by holding it on the Clearview Database. This processing is carried out by Clearview at its own instigation, in order to be able to offer a service to its customers. The Commissioner understands that Clearview's customers are not involved in any way in the scraping of data by Clearview or in the construction of the Clearview Database. For instance, Clearview's customers do not give it instructions, or express preferences, as to the types of images that should be represented in the Clearview Database. The techniques and technology that are used in order to create the Clearview Database are entirely for Clearview to determine.

42. It follows from the above that Clearview is *sole data controller* in relation to Activity 1 Processing.

43. Activity 2 Processing consists of Clearview's processing of Probe Images submitted to Clearview by its customers, and the provision by Clearview to its customers of search results in relation to those Probe Images. This processing takes place when Clearview receives a Probe Image from a customer, and compares it with the Clearview Database (by comparing the Probe Vectors derived from the Probe Image with the Database Vectors derived from the Database Images) in order to generate a list of results for the customer.

44. In more detail, Clearview's Activity 2 processing consists of:

- The matching of the Probe Image against the Clearview Database. This constitutes processing of: (i) the personal data contained in the Probe Image; and (ii) the personal data of *all* of those whose images are contained in the Clearview Database (since all of those individuals are being considered as potential matches for the Probe Image); and (iii) in particular, the personal data of any individuals whose images are identified as potential matches for the Probe Image.

- The provision of search results to the customer. This constitutes processing of: (i) the personal data contained in the Probe Image; and (ii) the personal data contained in or associated with any images that are identified as potential matches for the Probe Image and that are therefore included in the search results provided to the customer.

45. In relation to its Activity 2 Processing, Clearview is in each case a controller (as is the customer that submitted the Probe Image in question). This is for the following reasons.

- The Clearview service is not made generally available, but is only offered to specific types of customer (such as law enforcement organisations). The service will be made available only where the purposes for which the customer wishes to submit Probe Images, are consistent with the purposes for which Clearview is willing to make its service available. It follows that the customer and Clearview are each involved in

determining the purposes for which personal data is processed in the context of Activity 2.

- Likewise, the customer and Clearview are each involved in determining the means of processing: the service offered by Clearview is designed and created by Clearview, but it is the customer that chooses to use that service.

It follows from the above that Clearview is a controller (along with its customer) in respect of Activity 2 Processing.

Clearview's processing of the personal data of UK residents comes within the scope of the GDPR and UK GDPR

46. The Commissioner has considered carefully whether the Clearview's processing of personal data comes within the scope of the GDPR and UK GDPR, and hence whether it comes within the jurisdiction of the Commissioner.

47. In this respect, the Commissioner has had regard to the extensive submissions in the Representations to the effect that the Commissioner lacks jurisdiction over Clearview's processing: see paragraph 8 of the Representations (summarising Clearview's case in this regard), and paragraphs 47-91 of the Representations (setting out the case in detail). The Commissioner does not accept that he lacks jurisdiction.

48. The Commissioner considers that Clearview' s processing (that is, both its Activity 1 and Activity 2 processing) comes within Article 3(2)(b) GDPR and UK GDPR, as follows.

(1) Both Activity 1 and Activity 2 processing by Clearview of the personal data of data subjects resident in the UK, taking place prior to the end of the Brexit implementation period, came within Article 3(2)(b) GDPR.

(2) Both Activity 1 and Activity 2 processing by Clearview of the personal data of data subjects resident in the UK, taking place after the end of the Brexit implementation period, came within (and continue to come within) Article 3(2)(b) UK GDPR.

49. *First*, Clearview's Activity 1 Processing of the personal data of data subjects resident in the UK, and taking place prior to the end of the Brexit implementation period, came within Article 3(2)(b) GDPR, since that processing related to the monitoring of the behaviour of UK data subjects taking place within the UK. This is for the following reasons.

(1) As explained above, the purpose of Clearview's Activity 1 Processing is to enable Clearview to provide a service to its customers, by enabling those customers to match Probe Images with the images on the Clearview Database.

(2) By seeking to match Probe Images in this way, customers are "monitoring" the behaviour of those who appear in the Probe Images. They are seeking to identify and/or to find out more about the individuals who appear in the Probe Images. Those individuals are likely to be of interest to law enforcement because of their behaviour or suspected behaviour; i.e they may be criminal suspects, and/or the Probe Image itself may show them as engaged in apparent criminal activity.

(3) Customers are likewise monitoring the behaviour of the individuals whose images appear on the Clearview Database, where those individuals are identified as a potential match for the Probe Image. By considering the search results from the Clearview Database, and/or by considering those search results in conjunction with the Probe Image, customers may be able to ascertain information about a particular individual's behaviour, not only at a particular point of time, but extending over a period of time. Obtaining or seeking to obtain information of this nature would constitute monitoring.

(4) By reason of the factual findings set out at paragraphs 21-32 above, it is inevitable that a substantial number of those whose behaviour is monitored in this way by Clearview's customers will be data subjects resident in the UK.

(5) Just as Clearview takes no steps to exclude data subjects *resident* in the UK from the Clearview Database, so likewise it takes no steps to exclude images of the *behaviour* of such data subjects in the UK from the Clearview Database. Hence it is inevitable, not merely that Clearview's customers will monitor the behaviour of a substantial number of UK data subjects, but that they will monitor the behaviour *in the UK* of a substantial number of such data subjects. The Commissioner relies in this regard on the matters set out at paragraphs 21-32 above.

(6) Clearview's Activity 1 Processing is *related to* the monitoring that is carried out by Clearview's customers as

described above. Such monitoring by Clearview's customers could not take place without Clearview's Activity 1 Processing. Indeed, the very purpose of Clearview's Activity 1 Processing is to enable Clearview to provide its image matching service to its customers, thereby enabling the monitoring carried out by Clearview's customers to take place.

50. *Secondly*, Clearview's Activity 2 Processing of the personal data of data subjects resident in the UK, and taking place prior to the end of the Brexit implementation period, came within Article 3(2)(b) GDPR. This was the case, regardless of whether or not such processing took place in the course of providing services to a Clearview customer established in the UK.

(1) Clearview's Activity 2 processing consists of the matching of the Probe Image against the Clearview Database, and the provision of search results by Clearview to its customer.

(2) By seeking to match Probe Images against the images in the Clearview Database, Clearview's customers are monitoring the behaviour of UK residents in the UK. Paragraphs 49(2)-(5) above are repeated.

(3) Clearview's Activity 2 processing is *related* to the monitoring that is carried out by Clearview's customers as described above. The very purpose of Clearview's Activity 2 processing is to provide Clearview's image matching service to its customers, thereby enabling the monitoring carried out by Clearview's customers to take place.

(4) Without prejudice to the generality of the points made above, Clearview's Activity 2 processing in connection with the UK Test Phase came within Article 3(2)(b) UK GDPR. It is highly likely that a significant number of Probe Images submitted by UK law enforcement agencies during the UK Test Phase would have related to UK residents, and to the behaviour of UK residents in the UK.

51. *Thirdly*, Activity 1 Processing of the personal data of data subjects resident in the UK, and taking place after the end of the Brexit implementation period, comes within Article 3(2)(b) UK GDPR.

52. The Commissioner understands that such Activity 1 Processing has continued after the end of the Brexit implementation period, and is still continuing. This is so, regardless of the fact that the UK Test Phase was completed before the end of the Brexit implementation period. Clearview continues: (a) to hold the personal data of data subjects resident in the UK on the Clearview Database; and (b) to collect the personal data of such data subjects and to add it to the Clearview Database. Such processing comes within Article 3(2)(b) UK GDPR: the same reasoning as is set out at paragraph 49 above would apply in respect of such processing.

53. *Fourthly*, Activity 2 Processing of the personal data of data subjects resident in the UK, and taking place after the end of the Brexit implementation period, comes within Article 3(2)(b) UK GDPR.

54. The Commissioner understands that such Activity 2 Processing has continued after the end of the Brexit implementation period, and is still continuing. Although Clearview has not offered its services to

customers established in the UK after the end of the Brexit transition period, it has continued to offer its services to other customers. In so doing, it has processed the personal data of: (a) UK residents whose images have been submitted as Probe Images; and (b) UK residents whose images (and associated data) are held on the Clearview Database, including (but not limited to) UK residents whose images have been identified as a potential match for Probe Images. Such processing comes within Article 3(2)(b) UK GDPR: the same reasoning as is set out at paragraph 50(1)-(3) above would apply in respect of such processing.

55. The Commissioner notes that the French data protection regulator (CNIL) has taken a similar position, as regards the question whether CNIL has jurisdiction over Clearview's processing, and whether Clearview's processing of the personal data of data subjects in the European Union (and in particular in France) comes within the scope of Article 3(2)(b) GDPR: see CNIL's Decision Number MED 2021-134 of 1st November 2021, issuing an order to comply to Clearview.

56. In the Representations, Clearview contends that Article 3(2)(b) GDPR and UK GDPR cannot apply to processing carried out by Clearview, since any "monitoring" of data subjects is carried out not by Clearview but by its customers (see e.g. paragraphs 68-79 of the Representations). The Commissioner does not accept that the application of Article 3(2)(b) is limited in this way, in particular given the very close relationship between (a) the creation and maintenance of the Clearview Database, and the operation of Clearview's services, and (b) the activities of Clearview's customers involving the monitoring of data subjects.

57. Clearview also contends that the extra-territorial effect of Article 3(2)(b) GDPR and UK GDPR should be narrowly construed.

However, the effect of Clearview's proposed construction is that processing that involves the scraping of personal data from the internet across the entire world falls outside the jurisdiction of the UK regulator (or any EU regulator) *unless* the controller is itself established in the UK or EU). This enables a controller to evade effective regulatory scrutiny for such processing – notwithstanding its potential impact on UK or EU data subjects - by choosing to establish itself in a jurisdiction where the protection for personal data is more limited than that provided by the GDPR or UK GDPR. The Commissioner considers that such a construction is inconsistent with the purposes of the GDPR and UK GDPR, in particular their purpose of providing a high degree of protection to data subjects.

Clearview's processing has infringed the GDPR and UK GDPR and continues to infringe the UK GDPR

58. In relation to the processing of personal data falling within the GDPR or UK GDPR, Clearview has infringed the GDPR or UK GDPR, and continues to infringe UK GDPR, in numerous respects as set out below.

59. The Commissioner notes that the Representations, while addressing in detail the contention that Clearview's processing falls outside the Commissioner's jurisdiction, do not put forward an alternative case that (if the GDPR and UK GDPR are applicable) Clearview has not been and is not in breach. Evidently (and rightly) Clearview accepts that if the GDPR and UK GDPR are applicable then any contention that it has complied with their provisions would be hopeless.

60. ***First***, the processing in question has infringed Article 5(1)(a) GDPR and UK GDPR, and continues to infringe Article 5(1)(a) UK GDPR. The processing is not, and has not been, fair, lawful, or transparent.

61. As to the *fairness* of the processing in question, the processing is unfair given that data subjects are not made aware of the processing and would not reasonably expect their personal data to be processed in this way. Data subjects whose images are made available on the public facing internet would not expect their images to be scraped, added to a worldwide database, and made available to a wide range of customers (including law enforcement customers) for the purpose of matching images on the database against Probe Images.

62. To the extent that Clearview suggest that images on the public facing internet have been placed there voluntarily by the individuals who are shown in those images, and can therefore (without any unfairness) be collected and used for any purpose whatsoever, any such suggestion is wholly misconceived. In addition to the general points made above:

- Vast numbers of images on the public facing internet are placed there, not by the individuals shown in the images, but by third parties.

- Images placed on the public facing internet may subsequently be made private (e.g. where an individual places an individual on a social media site and subsequently changes their privacy settings). There is no indication whatsoever that Clearview

would remove an image from the Clearview Database following such a change of privacy settings.

63. As to the *lawfulness* of the processing in question, the processing: (a) does not meet any of the conditions for the lawful processing of personal data in Article 6 GDPR or Article 6 UK GDPR; and (b) does not meet any of the conditions for the lawful processing of special category personal data in Article 9(2) GDPR or Article 9(2) UK GDPR: see further below.

64. As to the *transparency* of the processing in question, the processing is not transparent given that: (a) it is and has been invisible to data subjects, since they are not made aware of the processing and would not reasonably expect their personal data to be processed in this way; and (b) Clearview has not and does not comply with the provisions of Article 14 GDPR and UK GDPR in relation to the provision of information to data subjects. Data subjects would not be aware of Clearview's processing unless they happened to come across Clearview's website (which describes the processing in general terms) and/or they happened to read reports about it in the media.

65. ***Secondly***, the processing is and has infringed Article 5(1)(e) GDPR and UK GDPR. Clearview does not have a data retention policy and hence cannot ensure that personal data is not held for longer than necessary. There is no indication in the Representations as to when (or whether) any images are removed from the Clearview Database. On the contrary, the evidence (as set out above) indicates that the scale of the Clearview Database continues to grow.

66. ***Thirdly***, the processing is and has infringed Article 6 GDPR and Article 6 UK GDPR. None of the bases for lawful processing set out

therein have been satisfied by Clearview. It is for Clearview to demonstrate that one or more of the bases in Article 6(1) GDPR and UK GDPR is met: see Article 5(2) GDPR and UK GDPR. Clearview has failed to do so. The Representations (rightly) do not attempt to argue that any of the bases in Article 6(1) GDPR or UK GDPR is or has been satisfied.

67. ***Fourthly***, the processing infringes, and has infringed, Article 9(1) GDPR and Article 9(1) UK GDPR. The personal data processed by Clearview constitutes "special category data": as set out above, Probe Vectors and Database Vectors constitute biometric data falling within Article 9(1) GDPR and UK GDPR (and the Representations do not suggest otherwise). None of the conditions set out in Article 9(2) GDPR or UK GDPR have been satisfied by Clearview in relation to its processing of special category personal data. It is for Clearview to demonstrate that one or more of the conditions in Article 9(2) GDPR and UK GDPR is met: see Article 5(2) GDPR and UK GDPR. Clearview has failed to do so. The Representations (rightly) do not attempt to argue that any of the bases in Article 9(2) GDPR or UK GDPR is or has been satisfied.

68. ***Fifthly***, the processing is and has infringed Article 14 GDPR and Article 14 UK GDPR. Clearview has not provided data subjects with the information set out therein, in respect of Clearview's processing of their personal data. The only way in which data subjects can obtain any of that information is by contacting Clearview and requesting it.

69. ***Sixthly***, the processing is and has infringed Articles 15, 16, 17, 21 and 22 GDPR and UK GDPR. Clearview has impeded and continues to impede the exercise of these rights since:

- Data subjects are not provided with the information specified in Article 14;

- In order to exercise these rights, data subjects need to provide Clearview with additional personal data, by providing a photograph of themselves that can be matched against the Clearview Database, which is itself a significant fetter on and disincentive to the exercise of those rights; and

- Although Clearview has previously operated a mechanism for allowing data subjects to seek to have their personal data removed from the Clearview Database, it has now ceased to do so (see Representations, paragraph 149).

70. ***Seventhly***, contrary to Article 35 GDPR and UK GDPR, Clearview has failed at any time to conduct a DPIA in respect of its processing of the personal data of UK residents. Nor is there any indication in the Representations that Clearview intends to do so at any point in the future.

Clearview's infringements warrant enforcement action by the Commissioner

71. The Commissioner considers that the infringements of UK GDPR by Clearview are significant and warrant enforcement action.

72. His reasons for this conclusion include the following.

- Clearview are highly likely to hold vast volumes of personal data, including about UK based data subjects.

- Clearview has not specifically confirmed how it obtains this information, other than that it has been scraped from the public facing internet.
- Clearview's processing of personal data is very largely invisible to data subjects, who would be unaware that their personal data has been scraped from the internet so that it can potentially be matched with images that are of interest to law enforcement bodies and other Clearview customers.
- There are extensive and continuing infringements of the UK GDPR. Clearview do not accept that the UK GDPR applies – notwithstanding that they are processing personal data about very significant numbers of UK residents – and consequently they have made no attempt whatsoever to comply with it.

73. The Commissioner therefore requires Clearview to take the steps set out in Annex 1.

74. The Commissioner considered, as he is required to do under section 150(2) DPA when deciding whether to serve an Enforcement Notice, whether any infringement has caused or is likely to cause any person damage or distress. There is clear potential for both damage and distress to be suffered by data subjects when their images are matched with a Probe Image, especially if the match turns out to be inaccurate and erroneous. There is the potential for a match to lead to an individual being arrested or charged with a criminal offence.

75. However, the Commissioner considers that compliance with the UK GDPR provisions referred to above to be a matter of central importance to data protection law. Even if a failure to comply has not, or is not likely, to cause any person damage or distress, the issue of this Enforcement Notice to compel compliance would

nonetheless be an appropriate exercise of the Commissioner's enforcement powers.

76. The Commissioner has considered whether it is practicable for Clearview to comply with the requirements of Annex 1. In this regard the Commissioner notes that, in the context of proceedings brought in the US District Court for the Northern District of Illinois (*Mutnick and Others v Clearview and Others*: Case No. 20 C 512) Clearview has stated in Court filings[2] that it has done the following:

- Blocked all photos in the database that were geolocated in Illinois from being searched;
- Constructed a 'geofence' around Illinois;
- Decided that it will not collect facial vectors from images that contain metadata associated with Illinois; and
- 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".

The Commissioner considers that by adopting comparable steps in relation to UK residents Clearview would be able to comply with the requirements set out in Annex 1.

77. Given that the US Court was willing to impose the requirements set out above, the Commissioner does not accept that the requirements set out in Annex 1 are not practicable. Further, the Commissioner notes that Clearview itself (whether in its Representations, or otherwise) has not put forward any alternative proposals as to how the Commissioner's concerns can be met: see e.g. paragraphs 105-108, which set out Clearview's contentions as

[2] Clearview AI Says It Will No Longer Provide Facial Recognition To Private Companies (buzzfeednews.com)

to why the Commissioner's requirements are said to be inappropriate. Clearview's position in its Representations appears to be that even if (contrary to its case) it is and has been in breach of GDPR and UK GDPR, no enforcement action whatsoever can or should be taken by the Commissioner in respect of that breach. This position is wholly unrealistic, and unacceptable.

78. Having regard to the significant nature of the infringement, the scale of the personal data being processed and the context in which it is processed, the Commissioner considers that this Enforcement Notice is a proportionate regulatory step to bring Clearview into compliance.

79. In relation to proportionality, the Commissioner notes the position adopted in the Representations, that compliance with the Commissioner's requirements would require Clearview to cease operating its service (see e.g. at paragraphs 93 and 96-104 of the Representations). The Commissioner does not seek to require this outcome: hence he is imposing the more limited and specific steps that are set out in Annex 1 and that are intended for the protection of UK data subjects.

80. The Commissioner has also had regard to the desirability of promoting economic growth, and the potential impact his Notice might have in this regard, as is required under section 108 of the Deregulation Act 2015 and the Economic Growth (Regulatory Functions) Order 2017

81. As indicated above, Clearview is a US-based enterprise. It is understood that no employees of the company are located in the UK and that all revenues are remitted to the US. Clearview previously offered access to its service to a number of UK law

enforcement agencies on a trial basis (as explained above) and it is understood no fee was charged for these trials. Further, it is understood that these trials have since ended and access to the platform from UK IP addresses has been removed. The Commissioner has no evidence of any current intention for Clearview to re-enter the UK market. Having regard to these circumstances, the proposed enforcement action is unlikely to have an impact on any measure of economic activity or growth in the UK, including employment and GDP.

Terms of this Notice

82. The Commissioner therefore exercises his powers under section 149 DPA to serve an Enforcement Notice requiring Clearview to take specified steps to comply with the GDPR. The specified steps are set out in Annex 1 of this Notice.

83. Consequences of failing to comply with an Enforcement Notice 38. If a person fails to comply with an Enforcement Notice the Commissioner may serve a penalty notice on that person under section 155(1)(b) DPA requiring payment of an amount up to £17,500,000 or 4% of an undertaking's total annual worldwide turnover whichever is the higher.

Right of appeal

84. By virtue of section 162(l)(c) DPA there is a right of appeal against this Notice to the First-tier Tribunal (Information Rights). If an appeal is brought against this Notice, it need not be complied with

pending determination or withdrawal of that appeal. Information about the appeals process may be obtained from:

General Regulatory Chamber
HM Courts & Tribunals Service
PO Box 9300
Leicester
LEl 8DJ
Telephone: 0203 936 8963
Email: grc@justice.gov.uk

85. Any Notice of Appeal should be served on the Tribunal within 28 calendar days of the date on which this Notice is sent.

Dated the 18th day of May 2022

Stephen Eckersley
Director of Investigations
Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

ANNEX 1

TERMS OF THE ENFORCEMENT NOTICE

THIS NOTICE REQUIRES CLEARVIEW TO TAKE THE FOLLOWING STEPS:

1. Within six months following the date of the expiry of the appeal period, delete any personal data of data subjects resident in the UK that is held in the Clearview Database. Without prejudice to the generality of this requirement, Clearview are to delete any images of UK residents that are held in their database, and any other data associated with such images (including URLs and metadata).

2. Within three months following the date of the expiry of the appeal period, refrain from any further processing of the personal data of data subjects resident in the UK. Without prejudice to the generality of this requirement, Clearview must:

   (a) Cease obtained or "scraping" any personal data about UK residents from the public facing internet;
   (b) Refrain from adding personal data about UK residents to the Clearview Database; and
   (c) Refrain from processing any Probe Images of UK residents, and in particular refrain from seeking to match such images against the Clearview Database.

3. Refrain from offering any service provided by way of the Clearview Database to any customer in the UK.

4. Not do anything in future that would come within paragraphs 1-3 above without first: (a) carrying out a DPIA compliant with Article

35 UK GDPR, and (b) providing a copy of that DPIA to the Commissioner.