DATA PROTECTION ACT 2018

ENFORCEMENT POWERS OF THE INFORMATION COMMISSIONER

MONETARY PENALTY 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**") has decided to issue Clearview with a penalty notice under s.155 Data Protection Act 2018 ("**DPA 2018**"). The penalty notice imposes an

administrative fine on Clearview, in accordance with the Commissioner's powers under Article 83 of the GDPR and the UK GDPR, and s. 155 DPA 2018. The amount of the penalty is £7,552,800 (equivalent to €9 million, using the rate of exchange as at 25 April 2022).

4. The penalty is issued in respect of Clearview's past and continuing infringements of:

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

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

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

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

(v) the requirement of Articles 15, 16, 17, 21 and 22 GDPR and 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 GDPR and UK GDPR.

Accordingly, this Notice is issued under section 155 DPA 2018, read with 149(2)(a), (b) and (c) DPA 2018 and Article 83 UK GDPR. The penalty relates to infringements of both the GDPR and UK GDPR.

5. This Notice explains the Commissioner's reasons for his decision to impose this penalty.

Legal Framework

6. The Commissioner is responsible for monitoring the application of UK GDPR, as provided for by Article 51 and 57(1)(a) UK GDPR.

7. By Article 58(2)(i) UK GDPR the Commissioner has the power to impose an administrative fine, in accordance with Article 83, in addition to or instead of the other corrective measures referred to in Article 58(2), depending on the circumstances of each individual case.

8. By Article 83(1) UK GDPR, the Commissioner is required to ensure that administrative fines issued in accordance with Article 83 are effective, proportionate and dissuasive in each individual case.

9. Article 83(2) UK GDPR provides that:

> *When deciding whether to impose an administrative fine and deciding on the amount of the administrative fine in each individual case due regard shall be given to the following:*
>
> > *(a) the nature, gravity and duration of the infringement taking into account the nature scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them;*
> >
> > *(b) the intentional or negligent character of the infringement;*

(c) any action taken by the controller or processor to mitigate the damage suffered by data subjects;

(d) the degree of responsibility of the controller or processor taking into account technical and organisational measures implemented by them pursuant to Articles 25 and 32;

(e) any relevant previous infringements by the controller or processor;

(f) the degree of cooperation with the supervisory authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement;

(g) the categories of personal data affected by the infringement;

(h) the manner in which the infringement became known to the supervisory authority, in particular whether, and if so to what extent, the controller or processor notified the infringement;

(i) where measures referred to in Article 58(2) have previously been ordered against the controller or processor concerned with regard to the same subject-matter, compliance with those measures;

(j) adherence to approved codes of conduct pursuant to Article 40 or approved certification mechanisms pursuant to Article 42; and

(k) any other aggravating or mitigating factor applicable to the circumstances of the case, such as financial benefits gained, or losses avoided, directly or indirectly, from the infringement.

10. The matters identified in Article 83(2)(a)-(k) UK GDPR are also set out in section 155(3) DPA 2018, and are referred to below as "the Statutory Factors".

11. Article 83(5) UK GDPR materially provides:

Infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to £17,500,000, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher:

(a) the basic principles for processing, including conditions for consent, pursuant to Articles 5, 6, 7 and 9;

(b) the data subjects' rights pursuant to Articles 12 to 22 …

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

13. Section 155 DPA 2018 ("**Penalty Notices**") provides that

(1) If the Commissioner is satisfied that a person—

(a) has failed or is failing as described in section 149(2) […],

the Commissioner may, by written notice (a "penalty notice"), require the person to pay to the Commissioner an amount in sterling specified in the notice.

(2) Subject to subsection (4), when deciding whether to give a penalty notice to a person and determining the amount of the penalty, the Commissioner must have regard to the following, so far as relevant—

(a) to the extent that the notice concerns a matter to which the GDPR applies, the matters listed in Article 83(1) and (2) of the GDPR.

14. Section 149(2) DPA 2018 defines the "first type of failure" by a controller, as follows:

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.

15. 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.

Article 3 GDPR made similar provision, but by reference to "the Union" rather than the United Kingdom.

16. 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.

17. 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).

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

- 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");

- 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").

19. 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.

20. 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.

21. 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.

22. 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 by the data subject to personal data; rectification of personal data; erasure of personal data; objection to the processing of personal data; and automated processing.

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

24. In relation to the provisions of the UK GDPR referred to at paragraphs 17-23 above, there is no material difference between the GDPR and the UK GDPR.

25. Schedule 21 to DPA 2018 materially provides as follows in respect of the relationship between the GDPR and UK GDPR, at paragraph 2:

On and after IP completion day, references in an enactment to the UK GDPR (including the reference in the definition of "the data protection legislation" in section 3(9)) include—

(a) the EU GDPR as it was directly applicable to the United Kingdom before IP completion day, read with Chapter 2 of Part 2 of this Act as it had effect before IP completion day.

"IP completion day" means 11PM GMT on 31 December 2020. The effect of this provision, read with the provisions from DPA 2018 set out above, is that the Commissioner has the power to impose a monetary penalty under DPA 2018 section 155 in respect both of infringements of the GDPR taking place prior to IP completion day, and infringements of the UK GDPR taking place thereafter.

Factual findings in relation to the service provided by Clearview

26. Clearview operates an algorithmic 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").

27. 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").

28. 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.

29. 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).

30. 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.

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

32. 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.

[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

33. 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.

34. 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.

35. 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 31 above – that the number of images held on the Clearview Database has continued to increase.

36. 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.

37. 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

38. 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)).

39. 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).

40. 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)).

41. 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.

42. Given the factual findings set out at paragraphs 26 – 37 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.

43. 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

44. 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.

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

46. 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.

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

48. 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.

49. 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.

50. 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

51. The Commissioner has considered carefully whether 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.

52. 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.

53. 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.

54. *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 26-37 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 26-37 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.

55. *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 54(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.

56. *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.

57. 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 54 above would apply in respect of such processing.

58. *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.

59. 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 55(1)-(3) above would apply in respect of such processing.

60. 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.

61. 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.

62. 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

63. 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.

64. 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.

65. ***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.

66. 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.

67. 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.

68. 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.

69. 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.

70. ***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.

71. ***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.

72. ***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.

73. ***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.

74. ***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).

75. ***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.

Imposition of a monetary penalty: consideration of the Statutory Factors

76. The Commissioner has considered the Statutory Factors both in deciding whether to issue a penalty and in determining the amount of the penalty.

77. For the reasons given below, the Commissioner is satisfied that (i) the infringements are sufficiently serious to justify issuing a penalty in addition to exercising his corrective powers by issuing an Enforcement Notice; and (ii) the infringements are serious enough to justify a significant fine.

78. The various Statutory Factors are addressed below in turn.

(a) the nature, gravity and duration of the infringement taking into account the nature scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them;

79. The infringement has continued from 25 May 2018 (the date when the GDPR came into effect), and is still continuing as at the date when this Notice is issued.

80. The UK Test Phase, as described above, involved the processing of personal data in approximately 721 different searches involving Probe Images. The Commissioner is aware that some of these were duplicate searches (i.e. in some instances the same Probe Image was searched on more than one occasion), but nevertheless considers that the figure of 721 searches gives an indication of the number of UK data subjects whose Probe Images were used during the Test Period.

81. It is likely that the personal data of many more UK data subjects was processed by Clearview, having regard to the matters set out above as to the number of images in the Clearview Database, and the likelihood that very many of these images are of UK data subjects.

82. In relation to the nature and gravity of the breach, the Commissioner took into account the invisible nature of the processing (as explained above), and also the fact that the processing involved special category data (consisting of biometric data).

83. The Commissioner also had regard to the Commissioner's Regulatory Action Policy (RAP) which states that novel or invasive technology causing a high degree of intrusion into the privacy of individuals can expect regulatory action at the "upper end of the scale".

84. The Commissioner took into account Clearview's statement that it had acted on requests from UK data subjects to exclude their images from future searches. The Commissioner considered that this was some degree of mitigation in relation to Clearview's processing. The

Commissioner notes, however, that this practice has now been discontinued by Clearview (see Representations, paragraph 149).

85. The Commissioner noted Clearview's representations that it only offered its services to criminal law enforcement agencies. The Commissioner is also aware of recent announcements by Clearview that it has offered its services to the Government of Ukraine in its conflict with Russia, including for the identification of Russian combatants and of the deceased on both sides[2]. This goes beyond the use of the service for criminal law enforcement purposes, and is an example of the potential for expanding the scope of Clearview's services, with an associated potential for escalating the risks to data subjects.

(b) the intentional or negligent character of the infringement

86. The Commissioner considered that Clearview's breach of the GDPR and UK GDPR was negligent.

87. The Commissioner notes Clearview's apparently sincerely held position (as set out in the Representations) that its processing of personal data falls outside the GDPR and UK GDPR. The Commissioner nevertheless considers that Clearview ought (at the very least) to have been aware that their processing of the personal data of very substantial numbers of UK data subjects – both in connection with the UK Test Phase, and in connection with the operation of the Clearview service more generally – gave rise to a

[2] See e.g. the story at bbc.co.uk/news/technology-61055319

very significant risk that the GDPR or UK GDPR applied. The Commissioner considers that Clearview failed to take any appropriate steps to consider or manage that risk. Clearview's position of acquiring images of UK data subjects without acknowledging its corresponding legal responsibilities was not satisfactory.

(c) any action taken by the controller or processor to mitigate the damage suffered by data subjects

88. The Commissioner notes that no images (and in particular no images of UK data subjects) have been deleted by Clearview from the Clearview Database. Personal data continues to be processed in a non-compliant manner and the resultant risks to data subjects continue to apply.

89. The. Commissioner also notes that Clearview's withdrawal from the UK market has lessened the potential impact on UK data subjects. The service continues to be offered to non-UK customers (including law enforcement agencies) and the risk remains that UK data subjects may be subjected to investigation or other measures, based on their identification (or misidentification) using the Clearview service.

(d) the degree of responsibility of the controller or processor taking into account technical and organisational measures implemented by them pursuant to Articles 25 and 32

90. The Commissioner notes that Clearview has implemented some organisational and technical measures to protect the data that it processes. These are set out in the Representations (see in particular at paragraphs 41-42 and 153 of the Representations).

91. Set against this, there are no measures implemented by Clearview to bring its processing into compliance with UK GDPR. Clearview continues to maintain its position that the processing is not subject to the provisions of UK GDPR.

(e) any relevant previous infringements by the controller or processor

92. There is no relevant previous infringement.

(f) the degree of cooperation with the supervisory authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement

93. The Commissioner has taken account of paragraph 154 of the Representations in this regard. He accepts that Clearview responded to the Commissioner's inquiries in a timely manner, and provided a response to all of the Commissioner's sets of enquiries. However, some of the specific responses did not answer all of the questions asked and instead restated Clearview's position on jurisdiction.

(g) the categories of personal data affected by the infringement

94. Special category data was affected, as explained above. Children's data may also have been affected.

(h) the manner in which the infringement became known to the supervisory authority, in particular whether, and if so to what extent, the controller or processor notified the infringement

95. The incident became known to the Commissioner through a proactive investigation.

(i) where measures referred to in Article 58(2) (powers - see annexe 3) have previously been ordered against the controller or processor concerned with regard to the same subject-matter, compliance with those measures;

96. Not applicable.

(j) adherence to approved codes of conduct pursuant to Article 40 or approved certification mechanisms pursuant to Article 42;

97. Not applicable.

(k) any other aggravating or mitigating factor applicable to the circumstances of the case, such as financial benefits gained, or losses avoided, directly or indirectly, from the infringement.

98. There are no further relevant factors under this heading.

Decision to impose a penalty

99. Having regard to the combined effect of the various Statutory Factors, as set out above, the Commissioner considers that the imposition of a monetary penalty (in addition to the service of an Enforcement Notice) is an appropriate and proportionate exercise of the Commissioner's regulatory functions. The Commissioner has considered paragraphs 118-126 of the Representations (which assert that it is disproportionate for the Commissioner to both issue an Enforcement Notice and a Monetary Penalty Notice): having regard to the Statutory Factors, as set out above, the Commissioner does not accept that this is the case.

100. In reaching his conclusion that a monetary penalty should be imposed, 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.

101. 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, this Notice is unlikely to have

an impact on any measure of economic activity or growth in the UK, including employment and GDP.

Amount of the penalty

102. The Commissioner has given further consideration to the amount of the penalty, following receipt of the Representations.

103. The Commissioner has decided to impose a penalty of £7,552,800 (Seven Million, Five Hundred, Fifty Two Thousand and Eight Hundred Pounds), which is equivalent to €9 million.

104. The amount of the penalty has been determined in accordance with the C Commissioner's Regulatory Action Policy ("RAP") and applying the various sequential steps set out in the RAP. In determining the amount of the penalty the Commissioner has taken into account the various Statutory Factors addressed above.

105. **Step 1** is an initial element removing any financial gain to Clearview resulting from the infringements.

106. The Commissioner is unable to identify any specific financial gain to Clearview resulting from the infringements. The service is evidently operated by Clearview on a commercial basis and for financial gain. That said, the Commissioner does not have any figures for Clearview's income, or turnover. Clearview has expressly refused to

provide this information: see paragraphs 129-131 of the Representations.

107. Rather than seeking to reach an estimate as to financial gain, the Commissioner has decided not to set any "initial element" at Step 1.

108. Given that the calculation of the monetary penalty is not based on any assessment by the Commissioner as to Clearview's turnover, the points made at paragraphs 127-133 with regard to the Commissioner's allegedly capricious estimation of turnover are not material.

109. For the avoidance of doubt, the Commissioner does not consider that Clearview's continuing refusal to provide any figures as to its turnover can in any way preclude the Commissioner from imposing a monetary penalty and calculating the appropriate amount of the penalty.

110. **Step 2** is an element to censure the breach based on its scale and severity and taking into account the Statutory Factors. The Commissioner's consideration of Step 2 started with item (a) of the Statutory Factors (i.e. a consideration of the nature, gravity and duration of the failure). The Commissioner had regard to range of penalties available to him, and set an initial amount at just below the mid-point of this range, amounting to £7,552,800 (equivalent to €9 million).

111. The Commissioner has considered the other Statutory Factors, as set out above. The Commissioner does not consider that any of these justified either an increase or a reduction from the initial starting-point.

112. The Commissioner has also considered **steps 3, 4 and 5 of the RAP** (namely, adding in an element to reflect any aggravating factors, adding in an amount for deterrent effect to others and reducing the amount to reflect any mitigating factors including financial hardship). The Commissioner does not consider that any of these steps justify either an increase or a reduction from the figure of €9 million.

113. The Commissioner considers that a penalty at this level would be effective, proportionate and dissuasive, particularly in its deterrent effect on others with similarly novel technology having an impact on UK data subjects.

114. The Commissioner notes the position taken in the Representations that the Commissioner had not convened a panel of non-executive advisers to make a recommendation as to penalty. The Commissioner notes that the RAP states that this may be done in cases where the penalty is over £1 million, but that the RAP does not require this step to be taken. Further, the non-executive panel has not been convened in previous enforcement cases where the proposed penalty was of considerable size.

Summary and penalty amount

115. For the reasons above, the Commissioner considers that the infringement was an extremely serious failure. He is mindful that the penalty must be effective, proportionate and dissuasive. Taking all of the above factors into account, the Commissioner has decided to impose a penalty in the sum of £7,552,800 (equivalent to €9 million, using the rate of exchange as at 25 April 2022).

Payment of the penalty

116. The penalty must be paid to the Commissioner's office by BACS transfer or cheque by **17 June 2022** at the latest. The penalty is not kept by the Commissioner but will be paid into the Consolidated Fund which is the Government's general bank account at the Bank of England.

117. There is a right of appeal to the First-tier Tribunal (Information Rights) against:

(a) The imposition of the penalty; and/or,
(b) The amount of the penalty specified in the penalty notice

118. Any notice of appeal should be received by the Tribunal within 28 days of the date of this penalty notice.

119. The Commissioner will not take action to enforce a penalty unless:

- the period specified within the notice within which a penalty must be paid has expired and all or any of the penalty has not been paid;

- all relevant appeals against the penalty notice and any variation of it have either been decided or withdrawn; and

- the period for appealing against the penalty and any variation of it has expired.

120. In England, Wales and Northern Ireland, the penalty is recoverable by Order of the County Court or the High Court. In Scotland, the penalty can be enforced in the same manner as an extract registered decree arbitral bearing a warrant for execution issued by the sheriff court of any sheriffdom in Scotland.

121. Your attention is drawn to Annex 1 to this Notice, which sets out details of your rights of appeal under s.162 DPA.

Dated the 18th day of May 2022

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

Rights of appeal against decisions of the commissioner

1. Section 162 of the Data Protection Act 2018 gives any person upon whom a penalty notice or variation notice has been served a right of appeal to the First-tier Tribunal (Information Rights) (the 'Tribunal') against the notice.

2. If you decide to appeal and if the Tribunal considers:-

   a) that the notice against which the appeal is brought is not in accordance with the law; or

   b) to the extent that the notice involved an exercise of discretion by the Commissioner, that he ought to have exercised his discretion differently,

   the Tribunal will allow the appeal or substitute such other decision as could have been made by the Commissioner. In any other case the Tribunal will dismiss the appeal.

3. You may bring an appeal by serving a notice of appeal on the Tribunal at the following address:

   GRC & GRP Tribunal

   PO Box 9300

   Arnhem House

   31 Waterloo Way

   Leicester

   LE1 8DJ

Telephone: 0203 93 68 963

Email: grc@justice.gov.uk

a) The notice of appeal should be sent so it is received by the Tribunal within 28 days of the date of the notice.

b) If your notice of appeal is late the Tribunal will not admit it unless the Tribunal has extended the time for complying with this rule.

4. The notice of appeal should state:-

a) your name and address/name and address of your representative (if any);
b) an address where documents may be sent or delivered to you;
c) the name and address of the Information Commissioner;
d) details of the decision to which the proceedings relate;
e) the result that you are seeking;
f) the grounds on which you rely;
g) you must provide with the notice of appeal a copy of the penalty notice or variation notice;
h) if you have exceeded the time limit mentioned above the notice of appeal must include a request for an extension of time and the reason why the notice of appeal was not provided in time.

5. Before deciding whether or not to appeal you may wish to consult your solicitor or another adviser. At the hearing of an appeal a party may conduct his case himself or may be represented by any person whom he may appoint for that purpose.

6. The statutory provisions concerning appeals to the First-tier Tribunal (General Regulatory Chamber) are contained in sections 162 and 163 of, and Schedule 16 to, the Data Protection Act 2018, and Tribunal Procedure (First-tier Tribunal) (General Regulatory Chamber) Rules 2009 (Statutory Instrument 2009 No. 1976 (L.20)).