SUBMISSION TO THE INFORMATION COMMISSIONER

–

REQUEST FOR ASSESSMENT OF PROCESSING OPERATIONS BY CLEARVIEW AI, INC.

I. Introduction and Purpose of this Submission

1. Through this submission, Privacy International ("**PI**") provides the Information Commissioner's Office ("**ICO**") with evidence and analysis in order to assist its ongoing investigation into the compliance of Clearview AI, Inc. ("**Clearview**") with data protection legislation, in particular the General Data Protection Regulation ((EU) 2016/679) as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018 (the "**UK GDPR**"), and of its users with the Data Protection Act 2018 ("**DPA 2018**").

2. Clearview's data practices and uses of its platform give rise to substantial and ongoing breaches of the UK GDPR and DPA 2018. After introductory sections, this submission is structured around the two main stages of Clearview's impact on data subjects in the UK: (1) Clearview's initial processing of personal data through collection, storage and identification (section V), and (2) the use of Clearview's services by law enforcement authorities (section VI).

II. Privacy International

3. Privacy International is a non-profit, non-governmental organisation based in London, that works globally at the intersection of modern technologies and rights. Established in 1990, Privacy International undertakes research, litigation and advocacy to build a better future where technologies, laws and policies contain modern safeguards to protect people and their data from exploitation. As such, PI has statutory objectives which are in the public interest and is active in the field of the protection of data subjects' rights and freedoms. This submission relates to PI's ongoing work on corporate data exploitation, social media surveillance and facial recognition technology.

III. The Data Controller – Clearview AI, Inc.

4. Clearview AI, Inc. is a company based in the US, founded in 2017. Its sole product is a facial recognition platform allowing users to match photos of individuals to images of them found online. Its platform "includes the largest known database of 3+ billion facial images sourced from public-only web

sources, including news media, mugshot websites, public social media, and other open sources."[1]

5. In 2020, Clearview had about 2,900 active users. Despite directing all its publicly available marketing materials to law enforcement agencies, Clearview's clients reportedly ranged from "college security departments to attorneys general offices" and included "a startling number of private companies in industries like entertainment (Madison Square Garden and Eventbrite), gaming (Las Vegas Sands and Pechanga Resort Casino), sports (the NBA), fitness (Equinox), and even cryptocurrency (Coinbase)."[2] Sources also indicate private individuals have reportedly used "the app on dates and at parties – and to spy on the public".[3]

Technical description of Clearview's image database and product

6. According to our investigation and analysis of publicly available sources,[4] and our own technical expertise, we understand that the image database created by Clearview for its facial recognition platform is populated in four steps:

    1) **Automated image scraper** – an automated tool searches public webpages and collects any images that it detects as containing human faces. Along with these images, the scraper also collects metadata associated with these images, such as the image or webpage title, its source link and geolocation.[5]

    2) **Image and metadata storing** – the images and metadata collected through the scraping process are stored on Clearview's servers. These are stored indefinitely, i.e. even after a previously collected photograph or hosting webpage has been removed or made private.

    3) **Extraction of facial features through image processing neural networks** – for each image collected, every face contained in the image is scanned and processed in order to extract its uniquely identifying facial features. Faces are translated into numerical representations which we refer to as "vectors". These vectors consist of 512 data points that represent the various unique lines that make up a face. At this step, faces are converted from human

---

[1] 'Overview' (Clearview AI). Available at https://clearview.ai/overview.
[2] BuzzFeed News, 'Clearview's Facial Recognition App Has Been Used by The Justice Department, ICE, Macy's, Walmart, And the NBA' (27 February 2020). Available at https://www.buzzfeednews.com/article/ryanmac/clearview-ai-fbi-ice-global-law-enforcement.
[3] Kashmir Hill, 'Before Clearview Became a Police Tool, It Was a Secret Plaything of the Rich' (The New York Times, 5 March 2020). Available at https://www.nytimes.com/2020/03/05/technology/clearview-investors.html.
[4] Office of the Privacy Commissioner of Canada (OPCC), PIPEDA Report of Findings #2021-001 (2 February 2021). Available at: https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2021/pipeda-2021-001/; Clearview AI, 'Law Enforcement' (Clearview AI Website). Available at https://clearview.ai/law-enforcement; Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit, Letter to Clearview AI Inc. - Consultation prior to an order pursuant to Article 58(2)(g) UK GDPR (27 January 2021). Available at https://noyb.eu/sites/default/files/2021-01/545_2020_Anh%C3%B6rung_CVAI_ENG_Redacted.PDF.
[5] Clearview AI, Inc. Privacy Policy (version 1, last updated on 29 January 2020). Available at https://clearview.ai/privacy/privacy_policy. See also Exhibit 2, response to [redacted]'s Data Subject Access Request to Clearview AI, Inc.

recognisable images to machine-readable unique biometric numerical identifiers.

4) **Facial features storing and indexing/hashing** – Clearview stores vectors in a database on its server, where they are associated with the images and other scraped information. These vectors are then hashed (hashing consists of the transformation of a vector, through a mathematical function, into a shorter fixed-length value or key that represents the original vector), for two related purposes of indexing the database, and future identification of faces. Every photo of a face in the database has a different vector and respective hashed value associated with it to allow identification and matching.

7. The fifth and last step in Clearview's product lifecycle is **matching**. It is performed when a user of Clearview wishes to identify an individual, and for this uploads an image of their target and runs a search. Clearview's platform then analyses the image and extracts a vector from the target face, which is then hashed and compared against all hashed vectors previously stored in its database. Finally, the Clearview tool pulls any closely matching images from the vector database and shows them to the user as search results, along with any associated metadata, allowing the user to see the original source page of the matching images.

IV. Background

A. The Clearview "revelations" and subsequent interest from regulators

8. On 18 January 2020, a New York Times article entitled "The Secretive Company That Might End Privacy as We Know It" revealed Clearview's existence to the world.[6] Prior to this article, Clearview had operated with intentional secrecy, while offering its product to "more than 600 law enforcement agencies" and "at least a handful of companies for security purposes".[7] Following these "revelations", organisations and regulators in the United States (US) and abroad started scrutinising Clearview's practices.

9. In the US, "eight putative actions were filed within days of publication of the Times article, and more have followed".[8] Due to the lack of a federal privacy law in the US, these actions are taken in individual states under state legislation. One of these was filed in May 2020 by the ACLU in Illinois,[9] under the state's Biometric Information Privacy Act (BIPA), which regulates the collection and use of biometric information. Another was filed in February 2021 in California by civil

[6] Kashmir Hill, 'The Secretive Company That Might End Privacy as We Know It' (The New York Times, 18 January 2020). Available at https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html.
[7] Ibid.
[8] Sam Jungyun Choi et al, 'Clearview AI revelations spark action on use of facial recognition', Privacy Laws & Business International Report (August 2020). Available at https://www.cov.com/-/media/files/corporate/publications/2020/08/clearview-ai-revelations-spark-action-on-use-of-facial-recognition.pdf.
[9] ACLU, 'ACLU sues Clearview AI' (28 May 2020). Available at https://www.aclu.org/press-releases/aclu-sues-clearview-ai.

liberties activists and immigrants' rights groups, claiming that Clearview's practices violate the various local bans on government use of facial recognition technology.[10]

10. In Canada, the Office of the Privacy Commissioner of Canada ("**OPCC**"), together with provincial privacy regulators, opened an investigation into Clearview's practices in February 2020. It published its report of findings on 2 February 2021, recommending that Clearview (i) cease offering its services in Canada, (ii) "cease the collection, use and disclosure of images and biometric facial arrays collected from individuals in Canada", and (iii) "delete images and biometric facial arrays collected from individuals in Canada in its possession".[11]

11. In the UK and Australia, data protection regulators opened a joint investigation into the "personal information handling practices" of Clearview in July 2020.[12]

12. In the EU, disparate actions were taken in various countries. In Germany, an individual obtained from the Hamburg Data Protection Authority an advance notice of intent requiring Clearview to delete the hash value associated with his facial images.[13] The decision was limited to the individual case in issue and fell short of requiring the cessation of Clearview's activities in the jurisdiction. In Sweden, the Swedish Authority for Privacy Protection found in February 2021 that the Swedish Police Authority had unlawfully used Clearview's services and processed personal data in breach of the Swedish Criminal Data Act, the implementing legislation of the Law Enforcement Directive (2016/680) ("**LED**").[14] Various other countries opened investigations into Clearview's practices, such as Italy.[15]

13. The European Data Protection Board ("**EDPB**"), following questions from Members of the European Parliament raising concerns about Clearview, issued a preliminary assessment on 10 June 2020.[16] This assessment focused on "the compliance and lawfulness of processing resulting from the possible use by EU law enforcement authorities of a service such as offered by Clearview AI", expressing serious doubts.

---

[10] CNN Business, 'Clearview AI sued in California by immigrant rights groups, activists' (10 March 2021). Available at https://edition.cnn.com/2021/03/09/tech/clearview-ai-mijente-lawsuit/index.html.
[11] OPCC, para 111 (n 4).
[12] Information Commissioner's Office, 'The Office of the Australian Information Commissioner and the UK's Information Commissioner's Office open joint investigation into Clearview AI Inc.' (9 July 2020). Available at https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/07/oaic-and-ico-open-joint-investigation-into-clearview-ai-inc.
[13] noyb, 'Clearview AI's biometric photo database deemed illegal in the EU, but only partial deletion ordered' (28 January 2021). Available at https://noyb.eu/en/clearview-ai-deemed-illegal-eu.
[14] GDPRhub, 'IMY - DI-2020-2719' (11 February 2021). Available at https://gdprhub.eu/index.php?title=IMY_-_DI-2020-2719.
[15] Wired, 'Il Garante italiano della privacy indaga sulla più controversa società di riconoscimento facciale al mondo' (15 April 2021). Available at https://www.wired.it/attualita/tech/2021/04/15/riconoscimento-facciale-garante-privacy-clearview-ai/?refresh_ce=.
[16] EDPB, Letter to Members of the European Parliament (Ref: OUT2020-0052, 10 June 2020). Available at https://edpb.europa.eu/our-work-tools/our-documents/letters/edpb-response-meps-sophie-t-veld-moritz-korner-michal-simecka_en.

14. The number of different cases raised in Europe and elsewhere demonstrates keen and widespread concern from individuals and regulators about Clearview's practices. Yet to this date no efforts have been made to adopt a coordinated approach to this intrinsically global issue. A coordinated approach is long overdue in Europe, which boasts one of the strongest privacy and data protection frameworks in the world. A fragmented approach would detract from the value and force of the UK GDPR, EU GDPR and LED in bringing the same level of privacy protection to all residents of Europe.

B. Clearview's processing is subject to UK GDPR and the DPA 2018

15. PI submits that the controller's conduct satisfies Article 3(2) of the UK GDPR as Clearview has been, on several occasions, reported to offer its services to both private entities and law enforcement authorities in the UK, and has engaged in monitoring of the behaviour of data subjects within the UK by collecting their personal data. Moreover, previous versions of the company's website and its past conduct with regard to the exercise of data subjects' rights confirm that the company previously acted as being subject to the obligations imposed by the UK GDPR.

Clearview's targeting of customers triggers Article 3(2)(a) UK GDPR

16. First, in February 2020, BuzzFeed News reported that, according to documents seen by BuzzFeed News, the UK's National Crime Agency ("**NCA**"), the Metropolitan Police, the Northamptonshire Police, the North Yorkshire Police, the Suffolk Constabulary, the Surrey Police and the Hampshire Police, all had registered users with or had used or trialled the Clearview platform.[17] The documents indicated that the NCA used the software to carry out "a total of more than 500 searches, [...] while a number of users at the Met Police have run more than 170 searches between them since December [2019]".[18] In addition, Surrey Police admitted that it had used the technology on a "small number of occasions on a trial basis."[19] Both the Metropolitan Police[20] and the North Yorkshire Police[21] have neither confirmed nor denied that they have used the controller's software.

17. The aforementioned authorities fall within the definition of "competent authority" under section 30 and Schedule 7 of the DPA 2018, and their use of Clearview's product is therefore subject to the DPA 2018. In addition, having clients in the UK means Clearview has offered its services to data subjects in the UK.

---

[17] BuzzFeed News, 'More Than A Dozen Organizations From The Met Police To J.K. Rowling's Foundation Have Tried Clearview AI's Facial Recognition Tech' (28 February 2020). Available at https://www.buzzfeed.com/emilyashton/clearview-users-police-uk.
[18] Ibid.
[19] Ibid.
[20] Ibid. See also response from the Metropolitan Police Service to Freedom of Information Request Reference No: 01/FOI/21/018286 (29 April 2021), available at https://www.whatdotheyknow.com/request/733642/response/1781084/attach/html/3/attachment.docx.html.
[21] North Yorkshire Police, FOI disclosure log 1096.2019-20. Available at https://northyorkshire.police.uk/access-to-information/foi-disclosure-log/wish-to-request-information-about-the-use-of-facial-recognition-technology-in-your-police-force-1096-2019-20/.

18. Within the EU, the controller reportedly engaged "national law enforcement agencies, government bodies, and police forces in Belgium, Denmark, Finland, France, Ireland, Italy, Latvia, Lithuania, Malta, the Netherlands, Portugal, Slovenia, Spain and Sweden".[22]

19. Second, regardless of whether the controller's software was used by any or all of the aforementioned entities in those territories, it is clear that the controller intended to make its services available and promote them in Europe, potentially targeting both private entities and law enforcement authorities as customers. For example, a document obtained by BuzzFeed News via a public records request revealed that Clearview has been touting a "rapid international expansion" to prospective clients using a map that showcases how it either has expanded, or plans to expand.[23] The document indicates both the UK and EU countries as potential targets.

20. These reports and documents evidence "conduct on the part of the controller" demonstrating its "intention to offer goods or services to a data subject located in the United Kingdom", a key element in determining whether the Article 3(2)(a) targeting criterion has been met.[24]

Clearview's processing of personal data triggers Article 3(2)(b) UK GDPR

21. Third, the responses received from Clearview to Data Subject Access Requests ("**DSAR**") submitted under Article 15 of the EU GDPR (prior to the UK's European Union Exit date) show that it has collected personal data of data subjects in the UK and processed them in a way that triggers the application of Article 3(2)(b) UK GDPR. On 16 April 2020, PI staff member [redacted] (resident of the UK) submitted a Data Subject Access Request to Clearview via email, requesting "a copy of all [his] personal data [Clearview] process[es]" as well as answers to a series of questions under Article 15 of the EU GDPR. A copy of [redacted] correspondence with Clearview in relation to this DSAR can be found at Exhibit 1 to these submissions. The response that [redacted] received included a PDF file containing 3 photos of himself accompanied by a link to their online web source, and a short description of the third photo that accompanied it on the original website. It also linked to a webpage called "Clearview Data Policy", seemingly in response to [redacted]' additional questions but which did not address all of these questions.[25] Similarly, a DSAR submitted by PI staff member [redacted] resulted in Clearview providing a PDF file containing 8 photos of herself and associated metadata (including her name), along with the photo and name of a different individual seemingly

[22] BuzzFeed News (27 February 2020) (n 2).
[23] BuzzFeed News, 'Clearview AI Wants To Sell Its Facial Recognition Software To Authoritarian Regimes Around The World' (5 February 2020). Available at https://www.buzzfeednews.com/article/carolinehaskins1/clearview-ai-facial-recognition-authoritarian-regimes-22.
[24] EDPB, 'Guidelines 3/2018 on the territorial scope of the UK GDPR (Article 3) Version 2.1' (12 November 2019). Available at https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_3_2018_territorial_scope_after_public_consultation_en_1.pdf.
[25] Clearview Data Policy. Available at https://staticfiles.clearview.ai/clearview_data_policy.html.

erroneously picked up by Clearview's face search (redacted for purposes of this submission) (see Exhibit 2).

22. Clearview's response demonstrates that it systematically collects and processes, through its facial recognition algorithm, the personal data of data subjects who are in the UK. This practice amounts to monitoring data subjects' behaviour in the UK – it falls squarely within UK GDPR Recital 24's requirement that "in order to determine whether a processing activity can be considered to monitor the behaviour of data subjects, it should be ascertained whether natural persons are tracked on the internet including potential subsequent use of personal data processing techniques which consist of profiling a natural person".

23. Fourth, the controller's processing of UK and EU data subjects' personal data is indicated by the following elements from the controller's website: (a) a reference made to international transfers in a recent version of the controller's privacy policy: "When personal data is transferred outside the EEA, we will put in place suitable safeguards to ensure that such transfer is carried out in compliance with applicable data protection rules";[26] and (b) explicit references to the "General Data Protection Regulation" in the controller's Terms of Service and Privacy Policy.[27]

24. Fifth, following a complaint submitted by a data subject residing in Hamburg, the Hamburg Commissioner for Data Protection and Freedom of Information ("**HmbBfDI**") on 27 January 2021 communicated its intention to order Clearview to take certain steps to delete the data subject's data. The HmbBfDI asserted its own competence and application of the UK GDPR after concluding that Clearview does monitor the behaviour of data subjects in the Union, in particular noting that "it is the purpose of the company to be able to identify individuals. Such identification is possible by storing publications/profiles/accounts of users linked to a photograph, such as in particular in social networks, forums or blogs, in a profile, or at least being able to create a profile of an individual at any time. This subsequent use of personal data processing techniques aimed at profiling is a decisive indicator".[28]

25. In a case similar to the present one concerning the scraping of personal data by a controller with no establishment in the EU, the Dutch data protection authority ("**Autoriteit Persoonsgegevens**") asserted its jurisdiction over the controller locatefamily.com, which scrapes and shares EU residents' personal data such as addresses and names.[29]

26. We see no reason why the ICO should reach a different conclusion from the HmbBfDI and the Autoriteit Persoonsgegevens as to applicability of the UK GDPR, which follows the same principles as the EU GDPR.

---

[26] Clearview AI, Inc. Privacy Policy (version 1) (n 5).
[27] Clearview AI, Inc. Terms of Service. Available at https://clearview.ai/help/tos.
[28] Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit (n 4).
[29] Autoriteit Persoonsgegevens, Decision of 10 December 2020 against locatefamily.com. Available at: https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/20210512_boetebesluit_ap_locatefamily.pdf.

27. Finally, a previous version of Clearview's privacy policy showed that it openly submitted itself to jurisdiction of EEA DPAs: "Residents of the European Economic Area or of Switzerland who wish to submit a complaint or seek resolution of a dispute related to Clearview AI's processing of personal data may seek appropriate recourse free of charge by contacting the appropriate Data Protection Authority (DPA) in their respective country."[30] This privacy policy was replaced in March 2021 by a version that takes care not to reference residents of the EEA or European legislation,[31] seemingly so as to evade this submission argument. At the time of writing, the pre-March 2021 version of the privacy policy, as well as an "EU/UK/Switzerland Data Access Form" and "EU/UK/Switzerland/Australia Opt-Out" form, are still available online, though de-referenced from Clearview's website.[32] These two forms were previously available through a "Privacy Requests Form" page.[33] As there is no evidence that Clearview has changed its practices nor stopped processing personal data of residents of the UK and EU, we see no reason to think that jurisdiction over their practices has changed in any way. Even if they had, data collected while their previous policy was in place remains subject to the jurisdiction applied in that previous policy.

28. In addition, despite de-referencing the privacy request forms, in the background Clearview still knows that it is, and behaves as, bound by obligations to respond to these requests. Indeed, a data subject in Greece submitted a data access request through the forms on 24 March, after the forms were de-referenced. She followed up with Clearview a month later noting that the deadline to respond had passed, after which she received an email from privacy@clearview-ai.zendesk.com asking her to re-submit a picture of her face and a photo ID, and promising her request would be given priority. At the time of filing this complaint, this individual has not yet received the data she requested. Details of this correspondence can be found in the complaint filed with the Greek Data Protection Authority by Homo Digitalis.

29. For the reasons outlined above, PI submits that the ICO should consider the controller's conduct as falling within the scope of Article 3(2) of the UK GDPR. In light of this, Clearview is also required to appoint a representative in the UK under Article 27(1), as none of the exceptions under Article 27(2) apply.[34]

---

[30] Clearview AI, Inc. Privacy Policy (version 1) (n 26).
[31] Clearview AI, Inc. Privacy Policy (version 2, last updated on 20 March 2021). Available at https://clearview.ai/privacy-policy.
[32] See EU/UK/Switzerland Data Access Form, available at https://clearviewai.typeform.com/to/ePcsEp and EU/UK/Switzerland/Australia Opt-Out, available at https://clearviewai.typeform.com/to/zqMFnt.
[33] See Clearview AI, "Privacy Request Forms", available at Wayback Machine Internet Archive, https://web.archive.org/web/20210303033642/https://clearview.ai/privacy/requests.
[34] For similar decisions on the lack of a representative by EU data protection authorities, see Autoriteit Persoonsgegevens (n 29), and CNPD, 4 February 2020, available at https://gdprhub.eu/index.php?title=CNPD_-_3018).

30. In addition, in light of current debates and proposals for the regulation of biometric mass surveillance,[35] PI submits that existing privacy laws and data protection regulation are entirely sufficient to find Clearview's practices illegal. A regulation of biometric mass surveillance would be indeed required to provide legal clarity on the use of facial recognition technology in public spaces in limited, individual cases. But mass processing of biometric data by a private company squarely falls within existing legislation, which was designed to protect European citizens against precisely those kinds of practices.

C. Why the ICO should consider this submission

31. In a statement from 9 July 2020, the ICO reported the opening of a joint investigation into the personal information handling practices of Clearview with the Office of the Australian Information Commissioner.[36] PI welcomes the opening of this investigation and hopes that the detailed technical and legal analyses of Clearview's practices that fed into these submissions shall be of help to this ongoing investigation.

32. The use of Clearview's product raises significant concerns in respect of the use of facial recognition technology ("**FRT**") by both private and public entities. In the UK, as explained above, the Metropolitan Police[37] and the North Yorkshire Police[38] are still failing to acknowledge whether they have used Clearview, despite a statement by the former in October 2019 that it was not "currently sharing images with any third parties for the purposes of Facial Recognition".[39] The uncertainty and lack of transparency around the use of FRT in private and public spaces in the UK is unacceptable, considering the serious and unprecedented interference with privacy that this technology presents.

33. PI is concerned that allowing companies like Clearview to deploy, sell or offer facial recognition software to private clients and law enforcement authorities can fundamentally undermine individuals' data protection rights, by failing to adhere to the data protection principles and strict standards for processing imposed by the UK GDPR and DPA 2018. The way this technology works and is currently deployed furthers the very harms that the legislation was intended to remedy. If left unsanctioned, such practices may have onerous implications for our society as a whole. In the digital age, these include a chilling effect on individuals' participation in democratic processes through the Internet, constraints on the development of their socio-political identities, and "real-life" harms such as vulnerability to "stalking" and inability to conduct daily activities without fear from surveillance.

---

[35] European Commission, 'Proposal for a Regulation laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)', COM(2021) 206 final (21 April 2021).
[36] ICO (n 12).
[37] BuzzFeed News (28 February 2020) (n 17).
[38] North Yorkshire Police (n 21).
[39] Metropolitan Police, 'Report to the Mayor of London' (4 October 2019). Available at https://www.london.gov.uk/sites/default/files/040910_letter_to_unmesh_desai_am_report_re_kings_cross_data_sharing.pdf.

34. It is thus essential that the ICO provides clarity with regard to the interpretation of important UK GDPR provisions such as those pertaining to legal bases under Articles 6 and 9, so as to avoid the proliferation of companies whose business model seeks to distort fundamental privacy and data protection values.

35. PI further submits that it would be of great value for ICO to consider these submissions in coordination with EU data protection authorities, to which PI or its partners have filed similar submissions. While the UK has now left the EU and the cooperation and consistency mechanisms provided under the EU UK GDPR no longer apply to the UK, PI strongly urges the ICO to cooperate with authorities. PI submits that investigations into Clearview would greatly benefit from cross-border cooperation, and that effective enforcement requires a consistent cross-border approach. As will be further explained in section V.D below, Clearview's practices threaten the open character of the Internet and the numerous freedoms it enables. Due to the global nature of the Internet, preserving these essential characteristics requires a global approach with effect on the widest possible scale. For these reasons, PI warmly welcomes the ICO's efforts to address this issue on a cross-border basis by opening a joint investigation with the Australian Information Commissioner, and submits that these investigation and enforcement efforts would greatly benefit from further global cooperation.

V. Legal Framework and Concerns: Processing by Clearview AI, Inc. (UK GDPR)

36. This section of the submission sets out PI's concerns in relation to the first stage of Clearview's interaction with data subjects in the UK, namely its initial processing of personal data through collection, storage and facial features extraction. Our legal analysis and concerns are based on PI's investigations of publicly available sources about Clearview's technology, informed by PI's technological and legal expertise. The primary concerns are that (i) Clearview processes both non-sensitive personal data and special categories data, without a valid legal basis, and (ii) this processing is in breach of various data protection principles.

37. After demonstrating that Clearview processes personal data and sensitive personal data (section A), this section of the submission will set out the various breaches of the UK GDPR in Clearview's personal data collection, storage and identification practices, which fail to respect the following data protection principles provided in Article 5 of the UK GDPR:

    (a) Principle 1 – Lawfulness, fairness and transparency
        i. Transparency (section B)
        ii. Fairness (section C)
        iii. Lawfulness and Lawful Basis under Articles 6 and 9 of UK GDPR (legitimate interests and special categories of personal data) (section D)
    (b) Principle 2 – Purpose Limitation (section E)

A. Clearview processes personal data and special categories data

Clearview processes personal data as defined by Article 4(1) UK GDPR

38. Informed by the technical description of Clearview's product in section III above, PI submits that Clearview is engaged in the "processing of personal data wholly or partly by automated means" as provided by Article 2(1) UK GDPR.

39. First, the images that Clearview collects from publicly available Internet sources are personal data. Photographs fall squarely within the definition of personal data under Article 4(1) UK GDPR, especially as interpreted with the help of Recital 26 UK GDPR: "The principles of data protection should apply to all information relating to an identified or identifiable natural person. […] In determining whether a natural person is identifiable, account should be taken of all the means, such as uniqueness, reasonably likely to be used by the controller or by any other person to identify the natural person directly or indirectly." Owing to the uniqueness of a face, a photograph of a face necessarily enables, through "human" recognition, the identification of an individual. As demonstrated by Clearview's technology, it also necessarily enables identification through machine recognition.

40. Such a conclusion is also in line with the case law of the Court of Justice of the European Union ("**CJEU**"). The latter has held that "the image of a person recorded by a camera constitutes personal data within the meaning of Article 2(a) of Directive 95/46 inasmuch as it makes it possible to identify the person concerned".[40] The definition of personal data under Directive 95/46 is, in essence, the same as the one contained within Article 4(1) of the UK GDPR.

41. Second, the metadata that Clearview also collects, stores and associates with the images contains personal data. As can be seen from the results of a DSAR submitted by PI staff [redacted] (Exhibit 2), the "Image Index" provided under face results contain descriptions of the image and/or webpage where the image was found, and can contain personal data such as names of individuals – including that of a different individual, details of whom we have redacted. This also reaffirms that the photos collected by Clearview are personal data, as they can "indirectly" enable identification of a data subject – the controller has "the means which may likely reasonably be used in order to identify the data subject", which makes the individual indirectly identifiable, as per the CJEU in *Breyer*.[41]

42. Third, in its September 2019 judgment on the use of live automated facial recognition technology ("**AFR**") used by the South Wales Police Force ("**SWP**") the Divisional Court went as far as accepting that any biometric data that permit the "immediate identification of a person" do comprise personal data.[42] As the Court underlined:

> *[M]embers of the public caught on the CCTV cameras are sufficiently individuated because the AFR Locate equipment takes images of their faces,*

[40] Case C-212/13 *František Ryneš v Úřad pro ochranu osobních údajů* [2014] ECLI:EU:C:2014:2428, para 22.
[41] Case C-582/14 *Patrick Breyer v Bundesrepublik Deutschland* [2016] ECLI:EU:C:2016:779, para 48.
[42] *R (Bridges) v Chief Constable of South Wales Police* ([2019] EWHC 2341 (Admin)), para 125.

that information is processed to extract biometric facial data, which is itself processed by being compared with information being drawn from the watchlist. By its nature, the facial biometric data is information about a natural person. That person is identifiable in the sense required by the definition in the 1995 Directive and the DPA 1998 because the biometric facial data is used to distinguish that person from any other person so that the matching process can take place.[43]

43. While the judgment dealt with the deployment of AFR through cameras in public places, PI submits that the same conclusion applies to the facial recognition technology used by Clearview, which equally allows for the immediate identification of natural persons.

44. Fourth, this personal data is collected, stored, structured through indexing via vectors, and retrieved when a user performs a search. These are all operations that form part of the definition of "processing" under Article 4(2) UK GDPR.

Clearview processes biometric data as defined by Article 4(14) UK GDPR

45. Under Article 4(14) UK GDPR, "biometric data" is defined as "personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, **such as facial images**".

46. Clearview is therefore processing biometric data in at least two respects:

    (a) The facial images it collects from online sources are biometric data; and
    (b) Once vectors are created, they themselves become biometric data, as they are data resulting from "specific technical processing relating to the physical […] characteristics of a natural person, which allow or confirm the unique identification of that natural person".

Clearview processes special categories data as defined by Article 9(1) UK GDPR

47. Clearview systematically processes special categories data as defined by Article 9(1) UK GDPR. Under Article 9(1), special categories of personal data are defined to include "biometric data for the purpose of uniquely identifying a natural person". According to Recital 51 of the UK GDPR, "[t]he processing of photographs should not systematically be considered to be processing of special categories of personal data as they are covered by the definition of biometric data only when processed through a specific technical means allowing the unique identification or authentication of a natural person." While this provides that the photographs of faces that Clearview collects from online sources aren't necessarily special categories data, it also makes clear that these photographs become so as soon as they are processed through step 3 of Clearview's database building. The scanning of every face, extraction of its uniquely

[43] Ibid, para 124.

identifying facial features, and translation of these features into vectors, consist of "specific technical means allowing the unique identification […] of a natural person."

48. This conclusion is also in line with the Divisional Court's findings in *Bridges*, where it was held that "the operation of AFR Locate involves the sensitive processing of the biometric data of" individuals, regardless of whether their images are contained in any watchlists:[44]

> *the AFR software takes a digital image and processes it through a mathematical algorithm to produce a biometric template (i.e. of the member of the public who is not on the watchlist) which is then compared to other biometric templates (i.e. of those who are on the watchlist) in order to provide information about whether one image is like the other. That process of comparison could only take place if each template uniquely identifies the individual to which it relates. Although SWP's overall purpose is to identify the persons on the watchlist, in order to achieve that overall purpose, the biometric information of members of the public must also be processed so that each is also uniquely identified, i.e. in order to achieve a comparison. This is sufficient to bring processing of their biometric data within the scope of section 35(8)(b) of the DPA 2018.*[45]

49. In addition, the metadata collected, stored and associated to facial images can contain personal data that reveal "racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership", which are also special categories data in accordance with Article 9(1) UK GDPR. For example, facial images can be found on a churchgoers' association website, or on a trade union members' website, thereby associating uniquely identifiable individuals to such characteristics.

50. It should also be noted that Clearview processes the personal data of children whose facial images are available online,[46] processing of which is subject to even more onerous restrictions throughout the UK GDPR.[47]

B. Transparency and the right to information

51. Transparency is a core component of the first data protection principle, set out in Article 5(1)(a) UK GDPR and supported by the right to information in Articles 13 and 14. Recital 60 of the UK GDPR provides that "[t]he principles of fair and transparent processing require that the data subject be informed of the existence of the processing operation and its purposes." Under Article 14(3)(a), where

---

[44] *R (Bridges) v Chief Constable of South Wales Police* [2019] EWHC 2341 (Admin), para 133.
[45] Ibid.
[46] See letter from Edward J. Markey (United States Senator) to Mr. Hoan Ton-That (3 March 2020), p. 2, available at: https://www.markey.senate.gov/imo/media/doc/Markey%20Letter%20-%20Clearview%20II%203.3.20.pdf, citing Kashmir Hill and Gabriel J.X. Dance, 'Clearview's Facial Recognition App Is Identifying Child Victims of Abuse', (New York Times, 7 February 2020), available at https://www.nytimes.com/2020/02/07/business/clearview-facial-recognition-child-sexual-abuse.html.
[47] For example, Articles 8, 12(1), and 17(1)(f), and Recital 38.

personal data have not been obtained from the data subject, as is the case for Clearview's processing, the controller ought to provide the data subject with information "within a reasonable period after obtaining the personal data, but at the latest within one month".

52. Clearview displays on its website a Privacy Policy (the "**Policy**")[48] which was updated in March 2021 from an earlier version addressed to a global audience.[49] The new version removed reference to residents of the European Economic Area or of Switzerland. Yet, it expressly applies to "photos that are publicly available on the Internet" and the extraction of "geolocation and measurements of facial features for individuals in the photos" – meaning it necessarily applies to all individuals in the world who, knowingly or unknowingly, have their facial images on publicly available parts of the Internet, and therefore to UK residents.

53. Clearview fails to provide the required transparency in at least two respects. First, Clearview never notifies individuals that it is processing their personal data, so that affected individuals never get to read Clearview's privacy policy before or after their personal data has been processed. According to the Art 29 WP Guidelines on transparency,[50] "a central consideration of the principle of transparency […] is that the data subject should be able to determine in advance what the scope and consequences of the processing entails and that they should not be taken by surprise at a later point about the ways in which their personal data has been used." The surprise in Clearview's case is complete – the only way for a data subject to know their data has been processed is to read the various media reports about their practices and further reach out to Clearview.

54. Second, even if one were able to access the Policy at the appropriate time before or shortly after their data is processed, Clearview provides incomplete and misleading information. In the section "What Data Do We Collect?", it notes that it "collects photos that are publicly available on the Internet" and "may extract information from those photos including geolocation and measurements of facial features for individuals in the photos". This statement is incomplete and misleading in two ways: (1) it presents the extraction of information and measurements of facial features as a mere possibility (by using the word "may", which should be avoided in privacy policies[51]), while in reality this is an automatic process, and (2) it omits various other types of personal data that Clearview automatically collects, namely names and other data obtained from URLs, photo and webpage titles collected.

55. In addition, this new version of Clearview's privacy has removed information about the legal bases upon which Clearview relies for the processing of personal data. The previous version of Clearview's privacy policy referred to UK GDPR-

[48] Clearview Privacy Policy (version 2) (n 31).
[49] Clearview Privacy Policy (version 1) (n 26).
[50] Article 29 Data Protection Working Party, 'Guidelines on transparency under Regulation 2016/679' (17/EN WP260 rev.01, Adopted on 29 November 2017, Revised and Adopted on 11 April 2018). Available at https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227.
[51] Art 29 WP Guidelines on transparency (n 50), para 13.

specific legal bases such as legitimate interests or explicit consent.[52] Again in what can be perceived as an effort to evade UK GDPR jurisdiction, Clearview has removed essential information that must be provided when processing UK residents' personal data.

56. In various public statements,[53] Clearview seems to assume that any right to information is obliterated by the fact that the personal data obtained is publicly available, and that data subjects would have therefore "given up" this right by quietly acquiescing to their images being publicly available online. However, as this submission will further analyse and explain below in paragraphs 96-104, there are numerous reasons why this is false. It is therefore unacceptable for Clearview to assume full information and acquiescence by individuals to their facial images being processed in this way.

57. This lack of transparency, a violation of the UK GDPR in itself, also implies that an overwhelming majority of data subjects are not aware of Clearview's processing of their personal data and therefore cannot possibly exercise any of their data subject rights in relation to that processing.

C. Fairness and data subjects' reasonable expectations

58. Fairness is another component of the first data protection principle in Article 5(1)(a) UK GDPR. Core to fairness is that the data processing concerned should be in line with individuals' reasonable expectations: "fairness means that you should only handle personal data in ways that people would reasonably expect and not use it in ways that have unjustified adverse effects on them."[54]

59. Reasonable expectation of privacy is also a key principle in jurisprudence of the European Court of Human Rights (the "**ECtHR**"), which is used to assess whether there has been an interference with an individual's private life under Article 8 of the European Convention on Human Rights ("**ECHR**"). The ECtHR has on several occasions investigated whether individuals "had a reasonable expectation that their privacy would be respected and protected".[55] In its case law, the Court has underlined that no person could reasonably expect footage depicting sensitive aspects of their private life to be later released in the media, even if their actions are "already in the public domain"[56] and that the use of photographic equipment to capture and process individuals' biometric data for purposes other than originally anticipated by them cannot fall within their reasonable expectations of privacy.[57]

---

[52] Clearview Privacy Policy (version 1) (n 26).
[53] Such as CNN Business YouTube channel, 'Clearview AI's founder Hoan Ton-That speaks out [Extended interview]' (6 March 2020). Available at https://www.youtube.com/watch?v=q-1bR3P9RAw.
[54] ICO, 'Guide to the General Data Protection Regulation (UK GDPR) – Principle (a): Lawfulness, fairness and transparency'. Available at https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-UK GDPR/principles/lawfulness-fairness-and-transparency/#fairness.
[55] *Barbulescu v. Romania* [GC] App no 1496/08 (ECtHR, 5 September 2017), para 73.
[56] *Peck v. United Kingdom* App No 44647/98 (ECtHR, 28 January 2003), paras 61-62.
[57] *Perry v. United Kingdom* App No 63737/00 (ECtHR, 17 July 2003), para 41.

60. PI submits that data subjects' reasonable expectations are blatantly trampled by Clearview's practices. In its recent decision, the OPCC found that "individuals who posted their images online, or whose images were posted by third party(ies), had no reasonable expectations that Clearview would collect, use and disclose their images for identification purposes".[58] This is further supported by a survey conducted by the European Agency for Fundamental Rights, in which European citizens were consulted on their willingness to share different types of personal data with both governmental agencies and private companies.[59] Across the EU-27 countries, 94% of the surveyed explicitly stated they were not willing to share their facial images with private companies for identification purposes.

61. The practice of gathering and processing publicly available data from social media platforms, coined "social media intelligence" ("**SOCMINT**") or "social media monitoring", has been decried in recent years for concerns about its compatibility with reasonable expectations of privacy. As part of a consultation on the use of social media monitoring by the European Asylum Support Office, the European Data Protection Supervisor ("**EDPS**") considered that social media monitoring "involves uses of personal data that go against or beyond individuals' reasonable expectations. Such uses often result in personal data being used beyond their initial purpose, their initial context and in ways the individual could not reasonably anticipate."[60]

62. Clearview's processing is a particularly intrusive form of social media monitoring, which goes far beyond the consultation and analysis of publicly available information on an ad hoc basis. Clearview's automatic collection, storage and processing for extraction of biometric identifiers make it further removed from any reasonable expectations of data subjects and therefore in no way compatible with the principle of fairness. The application of facial recognition to the collection of data compounds the issue: in its letter to the European Parliament giving a preliminary opinion on the use of Clearview by law enforcement, the EDPB highlighted that facial recognition technology may "affect individuals' reasonable expectation of anonymity in public spaces".[61] By combining SOCMINT and FRT, the service that Clearview offers is effectively annihilating individuals' expectation that their lives and identities in their physical, private lives cannot be immediately connected to their lives and identities on the Internet.

Comparison with Google's search engine

63. Clearview has, in various public reports, often compared its service to Google's search engine, arguing that its service is merely a "face search engine" instead

---

[58] OPCC (n 4), Overview.
[59] European Union Agency for Fundamental Rights, 'Your rights matter: Data protection and privacy - Fundamental Rights Survey' (18 June 2020). Available at https://fra.europa.eu/en/publication/2020/fundamental-rights-survey-data-protection#TabPubSharingdataonline1.
[60] EDPS, 'Formal consultation on EASO's social media monitoring reports (case 2018-1083)' (Brussels, D(2019) 1961). Available at https://edps.europa.eu/sites/edp/files/publication/19-11-12_reply_easo_ssm_final_reply_en.pdf.
[61] EDPB letter to the European Parliament (n 16).

of a website search engine, using faces rather than words as search terms.[62] This comparison seems intended to show that Clearview's tool would fall within data subjects' reasonable expectation of privacy, as everyone is aware that their data is scraped by search engines. However, PI would like to provide some clarifications as to the technical processes performed by Google's and Clearview's platforms, which will show that they are fundamentally different.

64. Google's and Clearview's "search engines" both perform three distinct actions:

(a) Crawling – automatically accessing a website and obtaining data from that website;
(b) Indexing – downloading content from a webpage to the server of the search engine, thereby adding content to its "index"; and
(c) Listing – showing matching content in the search result pages.

65. At the crawling stage, a website owner can make use of a robots.txt file instructing web robots how to crawl pages on their website. This is a text file that allows webmasters to tell a search engine they do not want the contents of their page indexed, for example. Abiding by the robots.txt file is optional from a technical perspective, and can possibly be disregarded by crawlers. Platforms such as LinkedIn or Facebook have included such files on their webpages, and specifically forbid crawlers in their website terms and conditions.

66. Google gives webmasters control over what information from their page is indexed and listed on its search results, including the option to opt-out entirely. Clearview has stated that their image crawler is configured to respect whatever instructions are present in robots.txt files.[63] However, Clearview has indexed content from YouTube, Facebook, Twitter and Instagram.[64] YouTube explicitly forbids automated collection of any information that might identify a person, and scraping of any data except by "public search engines", such as Google's.[65]

67. Clearview does not therefore respect instructions not to crawl and scrape content from certain websites, and has for this reason been sued by various large platforms for violation of their policies.[66] A reason why crawling by Google is acceptable, while scraping by Clearview isn't, is that Google has been around since the early days of Web 2.0. Users of Web 2.0 have developed content and used the web knowing that Google existed, and would scrape and index their content. Clearview, on the other hand, swooped in over a decade after the social media boom, claiming legitimacy of scraping whatever data was put online by users during that decade, and processing it through FRT, which didn't exist a few years ago. This fundamentally goes against the principles of foreseeability and reasonable expectation.

---

[62] E.g. CNN Business, 'Clearview AI's founder Hoan Ton-That speaks out [Extended interview]' (n 53).
[63] OPCC (n 4), para 17.
[64] Hill (n 6).
[65] YouTube GB, 'Terms of Service'. Available at https://www.youtube.com/static?template=terms.
[66] Alfred Ng and Steven Musil, 'Clearview AI hit with cease-and-desist from Google, Facebook over facial recognition collection' (CNET, 5 February 2020). Available at https://www.cnet.com/news/clearview-ai-hit-with-cease-and-desist-from-google-over-facial-recognition-collection/.

68. The systematic and indiscriminate collection of individuals' facial images from the Internet therefore does not fall within individuals' reasonable expectations and violates the fairness principle. The issue of fairness is compounded by the absence of transparency and disrespect for individuals' right to information, and various other violations of data protection principles as further set out in this submission.

D. Lawfulness and Lawful Basis

69. The third component of the first data protection principle in Article 5(1)(a) of the UK GDPR is lawfulness, requiring that personal data be processed lawfully. Article 6 sets out an exhaustive list of legal bases upon which personal data can be processed.

70. In addition to requiring a legal basis under Article 6, the processing of "special categories" personal data is prohibited unless one of the conditions in the exhaustive list given at Article 9(2) UK GDPR is met. As Clearview is processing biometric data qualified as "special categories" data, it ought to have a valid legal basis under both Article 6 and Article 9 – rather than under one or the other.[67] It is quite clear from the previous version of Clearview's privacy policy[68] that this dual requirement wasn't well understood: in the section "Legal basis for processing", it provided legal grounds for processing personal data (taken from Article 6) separate from legal grounds for processing special categories of data (taken from Article 9). In addition, in public reports Clearview seems to believe that the argument "we only obtain data from publicly available sources" on its own provides justification for all of its processing.

71. This submission will now analyse the applicability of the most relevant legal bases for Clearview's processing under Article 6 and Article 9.

<u>Legitimate Interests – Article 6(1)(f) UK GDPR</u>

72. The main legal basis on which Clearview could rely, and on which it seems to rely, under Article 6 is "legitimate interests" (Article 6(1)(f)). This can be seen from the obvious inapplicability of other legal bases, and the fact that in the previous version of its privacy policy,[69] Clearview explicitly relied on such basis: "the processing is necessary for the legitimate interests of Clearview, and does not unduly affect your interests or fundamental rights and freedoms". The other bases on which it sought to rely only applied to data pertaining to users of its services. For example, the legal basis "necessary in order to protect the vital interests of the data subject or of another natural person" (Article 6(1)(d)) could

[67] For unequivocal support for this 'cumulative' view, see Article 29 Data Protection Working Party, 'Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC' (844/14/EN WP217 Adopted on 9 November 2014), p.14. See also Edward S Dove and Jiahong Chen, 'What does it mean for a data subject to make their personal data 'manifestly public'? An analysis of UK GDPR Article 9(2)(e)' (2021) Vol. 00, No. 0, International Data Privacy Law, 1, 2.
[68] Clearview Privacy Policy (version 1) (n 26).
[69] Ibid.

only potentially apply to the last stretch of processing in the Clearview tool's lifecycle, i.e. when used by a law enforcement authority in the context of investigation of an identified crime – it cannot justify all of the prior processing.

73. Recital 47 of the UK GDPR provides that the legitimate interests of a controller:

> *may provide a legal basis for processing, provided that the interests or the fundamental rights and freedoms of the data subject are not overriding,* ***taking into consideration the reasonable expectations of data subjects based on their relationship with the controller****. Such legitimate interest could exist for example where there is* ***a relevant and appropriate relationship between the data subject and the controller*** *in situations such as where the data subject is a client or in the service of the controller. At any rate the existence of a legitimate interest would need careful assessment including* ***whether a data subject can reasonably expect at the time and in the context of*** *the collection of the personal data that processing for that purpose may take place.* (emphases added)

74. While the 'legitimate interests' basis does allow for some flexibility on the part of controllers, this does not imply that it is without limits or can be moulded exactly to fit or justify any processing operation.[70] But this legal basis keeps being abused: a recent resolution of the European Parliament warns that the legitimate interests basis is "very often abusively mentioned as a legal ground for processing".[71] It goes on:

> *The European Parliament […] points out that controllers continue to rely on legitimate interest without conducting the required test of the balance of interests, which includes a fundamental rights assessment; is particularly concerned by the fact that some Member States are adopting national legislation to determine conditions for processing based on legitimate interest by providing for the balancing of the respective interests of the controller and of the individuals concerned, while the GDPR obliges each and every controller to undertake this balancing test individually, and to avail themselves of that legal ground […]*

Legitimate Interests Assessment

75. A controller who seeks to rely on the legitimate interests basis ought to carry out an assessment, and make that assessment available to affected data subjects.[72] Clearview has not made any legitimate interests assessment publicly available. In his correspondence with Clearview, [redacted] requested to see a Legitimate Interests Assessment, but received no response (see Exhibit 1).

---

[70] ICO, 'Guide to the General Data Protection Regulation (UK GDPR) – Lawful basis for processing – Legitimate interests'. Available at https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-UK GDPR/lawful-basis-for-processing/legitimate-interests/.
[71] European Parliament resolution of 25 March 2021 on the Commission evaluation report on the implementation of the General Data Protection Regulation two years after its application (2020/2717(RSP)), para 7.
[72] ICO (n 70).

76. Such a legitimate interests assessment ought to be conducted with regard to the three conditions laid down by Article 6(1)(f) and further explicated in CJEU judgments *Rigas Satiksme*[73] and *Fashion ID*[74]:

(1) **"The pursuit of a legitimate interest by the data controller or by the third party or parties to whom the data are disclosed" ("purpose")** – in Clearview's case, this would be a commercial interest, i.e. of providing a service to third parties in exchange for money. It is self-evident that companies cannot treat the sole pursuit of their business models or of profit as "legitimate interests". The legitimate interest of the third parties to whom the data are disclosed can be taken to be the identification of real-life individuals. Taking the most common Clearview client, a law enforcement agency, Article 6(1) of the UK GDPR explicitly provides that the legitimate interests legal basis "shall not apply to processing carried out by public authorities in the performance of their tasks". Taking any other Clearview client, i.e. private companies and individuals, the legitimacy of their interest is only speculative, and at best of a limited and certainly creepy nature. In any case, a future and undefined third-party interest cannot justify the original processing operations. In this case the collection, biometric processing and storage of individuals' images is performed before any client uses the data, and before one can even envisage what specific use Clearview's clients will make of it. As described by the Office of the Privacy Commissioner of Canada, Clearview's activities consist in nothing more than "the mass identification and surveillance of individuals by a private entity in the course of commercial activity".[75]

(2) **"The necessity of processing personal data for the purposes of the legitimate interests pursued" ("necessity")** – were Clearview to have a legitimate interest relevant to this assessment, this condition would require assessing whether Clearview's commercial benefit could be achieved by means less intrusive of data subjects' fundamental rights and freedoms, according to the principle that derogations and limitations in relation to the protection of personal data must apply only in so far as strictly necessary.[76] Having established that the interests of a law enforcement authority cannot be taken into account in this particular assessment, it cannot be argued that private clients of Clearview *need* to use the tool for their interests. The existence of less intrusive alternatives is crucial, as is the principle of data minimisation, according to which data shall be "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed".[77] For example, Clearview reports that banks can use their tool for security and background checks; but banks have been conducting such

[73] Case 13/16 *Rigas Satiksme* [2017] ECLI:EU:C:2017:336, paras 28-31.
[74] Case C-40/17 *Fashion ID* [2019] ECLI:EU:C:2019:629, para 95.
[75] OPCC (n 4), para 72.
[76] Cases C-92/09 and C-93/09 *Volker und Markus Schecke and Eifert* [2010] EU:C:2010:662, para 86; Case C-473/12 *IPI* [2013] EU:C:2013:715, para 39; Case C-212/13 *Ryneš* [2014] EU:C:2014:2428, para 28.
[77] C/Jorge Juan 6 28001 – Madrid. Available at https://edpb.europa.eu/sites/edpb/files/article-60-final-decisions/es_2010_10_right_to_erasure_transparency_and_information_decisionpublic_redacted.pdf.

checks without such a tool for decades. It is also difficult to understand why such checks could only be carried out on the basis of a facial image, rather than through other identifiers.

(3) **"That the fundamental rights and freedoms of the data subject whose data require protection do not take precedence" ("balance")** – this requires balancing the controller's interests and the effects of processing on the data subject. In the seminal case of *Google Spain*, the CJEU considered that processing of personal data such as that

> *carried out by the operator of a search engine is liable to affect significantly the fundamental rights to privacy and to the protection of personal data when the search by means of that engine is carried out on the basis of an individual's name, since that processing enables any internet user to obtain through the list of results a structured overview of the information relating to that individual that can be found on the internet – information which potentially concerns a vast number of aspects of his private life and which, without the search engine, could not have been interconnected or could have been only with great difficulty – and thereby to establish a more or less detailed profile of him.*[78]

The CJEU also concluded that "[i]n the light of the potential seriousness of that interference, it is clear that it cannot be justified by merely the economic interest which the operator of such an engine has in that processing."[79]

What the CJEU described here as constituting significant interference with individuals' fundamental rights is precisely what Clearview is doing, with factors that can only reinforce the seriousness of this interference: (a) with Clearview, one does not need an individual's name to produce search results, but only their face, which can be acquired by simply passing an individual in the street and taking their picture; and (b) in the case of Clearview, an individual cannot, without using Clearview's product themselves, know what information about them is available out there (whereas they can perform a search of their own name and other text identifiers through Google).

The Art 29 WP Opinion on Legitimate Interests[80] further sets out some of the factors to be considered when carrying out such a balancing test:

i. **"The nature and source of the legitimate interest"** – as explained in paragraph (1) above, Clearview's interest in processing is a purely commercial interest.

---

[78] Case C-131/12 *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González* [2014] ECLI:EU:C:2014:317, para 80.
[79] Ibid, para 81.
[80] Art 29 WP Opinion on Legitimate Interests (n 67), pp. 36-43. **PI notes that the EDPB is updating this opinion in order to address issues highlighted in the Commission's report adopted by the European Parliament resolution mentioned above (n 71), and that the updated opinion can only be expected to require a more, rather than less stringent assessment than that set out in this submission.**

ii. **"The impact on the data subjects"**, including:

- the nature of the data such as whether the processing involves data that may be considered sensitive or has been obtained from publicly available sources – Clearview processes biometric data, which is particularly sensitive data and as will be explained in paragraphs 96-104 below, the fact that the data was obtained from publicly available sources does not detract from its sensitive quality and need for privacy protections. The Art 29 WP noted that:

  > *it is important to highlight that personal data, even if it has been made publicly available, continues to be considered as personal data, and its processing therefore continues to require appropriate safeguards. There is no blanket permission to reuse and further process publicly available personal data under Article 7(f).*[81]

  While recognising that the fact that personal data is publicly available may be a relevant factor in favour of finding legitimate interests, it then warned that this would only be the case "if the publication was carried out with a reasonable expectation of further use of the data for certain purposes (e.g. for purposes of research of for purposes related to transparency and accountability)." As explained above in section C, by no stretch of the imagination can Clearview's processing fall within this reasonable expectation of further use.

- the way data are being processed (including whether the data are publicly disclosed or otherwise made accessible to a large number of persons, or whether large amounts of personal data are processed or combined with other data e.g. in case of profiling, for commercial, law enforcement or other purposes) – the data processed by Clearview is subject to being run through their facial recognition algorithm, which is a particularly intrusive type of processing. Any of Clearview's clients may access the data processed by Clearview. This is a vast, undefined and unlimited population. In addition, piecing together bits of information about an individual's private life as advertently or inadvertently disclosed on the Internet can lead to forming a very intrusive and intimate view of their lives, which could never have been achieved through manual online research or use of keyword search engines. Considering that such intelligence can be used to make decisions about arrests or criminal convictions, the impact can only be considered of the highest level.

- their reasonable expectations especially with regard to the use and disclosure of the data in the relevant context – as further explained in section C, Clearview's processing cannot fall within data subjects'

[81] Ibid, p. 39.

reasonable expectations with regard to the use and disclosure of the data.

- the status of the data controller and data subject, including the balance of power between the data subject and the data controller, or whether the data subject is a child or otherwise belongs to a more vulnerable segment of the population – the circumstances of Clearview's processing make the impact on data subjects particularly acute. As Recital 47 of UK GDPR makes clear, what is legitimate should turn at least in part on whether a legitimate interest is served due to the relationship between the controller and subject. Not only does Clearview have no relationship with the affected individuals, its existence and activities are entirely unknown to most data subjects. Combined with the unforeseeable use of its tool by law enforcement authorities and private entities around the world, these circumstances make the balance of power particularly unfavourable to data subjects. In addition, due to its indiscriminate practices, Clearview necessarily processes personal data of children and vulnerable segments of the population. This vulnerability is often compounded by these populations' lack of control over their online identities.

The Art 29 WP Opinion on Legitimate Interests considers that in cases where anticipating or establishing harm or damage to data subjects is especially difficult, "it is all the more important to focus on prevention and ensuring that data processing activities may only be carried out, provided they carry no risk or a very low risk of undue negative impact on the data subjects' interests or fundamental rights and freedoms".[82] Considering the very significant impact Clearview's processing can have on data subjects' rights and freedoms, PI submits that the ICO ought to adopt a particularly cautious approach and prevent such risky processing.

iii. **"Additional safeguards to prevent undue impact on the data subjects"**, including:

- data minimisation – Clearview's operating model relies on principles opposite to data minimisation. By indiscriminately collecting and processing data through its facial recognition algorithms, it is very much akin to bulk collection of datasets and mass surveillance.

- technical and organisational measures to ensure that the data cannot be used to take decisions or other actions with respect to individuals ('functional separation') – the ultimate purpose of Clearview's product is for decisions and actions to be taken with respect to individuals, which can have a substantial negative impact on their lives, as further explained in section VI.A below.

[82] Ibid, p.51.

- extensive use of anonymisation techniques, aggregation of data, privacy-enhancing technologies, privacy by design, privacy and data protection impact assessments – as explained in section B above, [redacted] received no response to his request for a copy of any data protection impact assessment carried out by Clearview. To our knowledge, no privacy-enhancing technologies or designs are integrated in Clearview's product. In any case, the very purpose of its product is to strip every individual with some (wilful or unintentional) online presence of the protection they can reasonably expect for their identity.

- increased transparency, general and unconditional right to opt-out, data portability & related measures to empower data subjects (issues which play "a crucial role in the context of Article 7(f)"[83]) – this requires the controller to "perform a careful and effective test in advance, based on the specific facts of the case rather than in an abstract manner, taking also into account the reasonable expectations of data subjects". Despite multiple opportunities such as their privacy policy, or the numerous data subject access requests they receive, to PI's knowledge, Clearview has never performed or shown performance of the balancing test. As explained above in section B, Clearview's activities exhibit a complete lack of transparency and accountability to data subjects. Clearview provides a limited right to opt out of processing, though it is unclear what opting out of processing would entail. Owing to the nature of Clearview's technology, it is likely that any opt out would only affect the return of results when a search is performed, and would not limit further collection of personal data and further processing through its facial recognition algorithms.

77. Using the above framework to analyse the applicability of the legitimate interests legal basis to Clearview's processing activities, it is clear that on every single factor, Clearview falls in the high risk, high negative impact category. In addition, the various "redeeming" factors at their disposition that would mitigate this impact are simply absent from their activities. And because any legitimate interest is at best a commercial interest, the balance lies against their processing being acceptable and granted a legal basis under Article 6(1)(f).

78. Some assessments of legitimate interests have been made by data protection authorities around Europe and indicate a very narrow interpretation of legitimate interests that certainly cannot extend to the type of systematic and indiscriminate processing carried out by Clearview. For example, in its decision No 35/2020,[84] the Litigation Chamber of the Belgian Data Protection Authority assessed whether the re-use of an individual's publicly available Facebook profile picture

[83] Ibid, p.43.
[84] Autorité de Protection des Données, Chambre Contentieuse, 'Décision quant au fond 35/2020 du 30 juin 2020' (Numéro de dossier : DOS-2019-01240). Available at https://www.autoriteprotectiondonnees.be/publications/decision-quant-au-fond-n-35-2020.pdf.

by a Belgian judicial authority to enforce a "ban on presence" fell within the authority's legitimate interests. It noted that:

> *The UK GDPR carries a significant limitation to the freedom to re-use publicly available personal data. The Litigation Chamber notes that the applicable principle is as follows: the fact that an individual's profile picture is freely available to the public does not mean that others can use it freely. The use of this picture is possible only if a valid legal basis exists.*[85]

It decided that the re-use of the individual's picture did fall within the legitimate interests legal basis, for the authority had a legitimate interest (the enforcement of its decision), for the realisation of which the processing was necessary (it couldn't be achieved by any other means, and the authority took care to blur the faces of other individuals in the picture). This legal basis was specific to the individual complaint and could not be extended indiscriminately. The care taken by the Belgian Data Protection Authority to authorise the specific and limited re-use of the complainant's profile picture demonstrates the utter disproportionality and unacceptability of allowing Clearview's systematic and indiscriminate collection and re-use of every single facial image available on the Internet.

79. Similarly, the Office of the Privacy Commissioner of Canada conducted their jurisdiction's equivalent to a legitimate interests assessment, and concluded:

> *It is our view that Clearview does not, in the circumstances, have an appropriate purpose, for:*
>
> *i. the mass and indiscriminate scraping of images from millions of individuals across Canada, including children, amongst over 3 billion images scraped world-wide;*
>
> *ii. the development of biometric facial recognition arrays based on these images, and the retention of this information even after the source image or link has been removed from the Internet; or*
>
> *iii. the subsequent use and disclosure of that information for its own commercial purposes;*
>
> *where such purposes:*
>
> *iv. are unrelated to the purposes for which the images were originally posted (for example, social media or professional networking);*
>
> *v. are often to the detriment of the individual (for example, investigation, potential prosecution, embarrassment, etc.); and*
>
> *vi. create the risk of significant harm to individuals whose images are captured by Clearview (including harms associated with misidentification or exposure to potential data breaches), where the vast majority of those individuals have never been and will never be implicated in a crime, or identified to assist in the resolution of a serious crime.*[86]

[85] Ibid.
[86] OPCC (n 4), para 76.

80. To complement and flesh out the above assessment of impact on data subjects, the following sections highlight three key aspects of the harm caused to data subjects by Clearview's tool: (a) the recognised risks of biometric data processing, (b) an inevitable chilling effect on fundamental rights, and (c) the particular harms to be envisaged for vulnerable communities.

(a) Risks of biometric data processing

81. Biometric data is considered to be special categories data because it is unique data, generated from characteristics of humans, such as fingerprints, voice, face, retina and iris patterns, hand geometry, gait or DNA profiles. It is in itself sensitive data, no matter where it comes from or how it is collected.[87] As found by the Office of the Privacy Commissioner of Canada:

> *Biometric information is distinctive, unlikely to vary over time, difficult to change and largely unique to the individual. Facial biometric data is particularly sensitive given that it is a key to an individual's identity, supporting the ability to identify and surveil individuals.*[88]

82. The ECtHR also found that:

> *A person's image constitutes one of the chief attributes of his or her personality, as it reveals the person's unique characteristics and distinguishes the person from his or her peers. The right to the protection of one's image is thus one of the essential components of personal development and presupposes the right to control the use of that image.*[89]

83. When adopted in the absence of strong legal frameworks and strict safeguards, biometric technologies pose grave threats to privacy and personal security, as their application can be broadened to facilitate discrimination, profiling and mass surveillance.[90] As it stands, with a tool like Clearview's, a person's faceprint can be used to find their name and social media accounts, and to combine that information with their physical presence in the street, the stores they visit, and the photos they or their friends post online – a massive extension of the mostly limited ways in which biometrics have been used until now. According to the United Nations Commissioner for Human Rights, "[r]ecording, analysing and retaining someone's facial images without her or his consent constitute interferences with a person's right to privacy."[91]

84. As it is inherently difficult or impossible to change, biometric data can identify a person for their entire lifetime. This makes the creation of biometric databases problematic, as risks would need to be anticipated far into the future – whether

---

[87] *S. and Marper v. UK* [GC], App nos 30562/04 and 30566/0 (ECtHR, 12 April 2008).
[88] OPCC (n 4), para 74.
[89] *Reklos and Davourlis v. Greece*, App No 1234/05 (ECtHR, 15 April 2009), para 40.
[90] Privacy International, 'Biometrics'. Available at: https://privacyinternational.org/learn/biometrics.
[91] Office of the United Nations High Commissioner for Human Rights ("OHCHR"), 'Impact of new technologies on the promotion and protection of human rights in the context of assemblies, including peaceful protests' (UN Doc A/HRC/44/24, 24 June 2020), para 33. Available at https://undocs.org/A/HRC/44/24.

that be a change in political situation or regime, a future data breach, or the development of technology meaning that biometrics can be used for new purposes, and could reveal more information about individuals than is currently possible. As such, the collection and storage of biometric data has the potential to be gravely abused.[92]

85. The Art 29 WP of Directive 95/46 already recognised some years ago the significance of biometric data processing: "Biometric data changes irrevocably the relation between body and identity, because they make the characteristics of the human body 'machine-readable' and subject to further use."[93] It already predicted the harm that would be raised by the extraction of biometric features from publicly available information, and precisely pre-empted Clearview's processing activities:

> *Photographs on the internet, in social media, in online photo management or sharing applications may not be further processed in order to extract biometric templates or enrol them into a biometric system to recognise the persons on the pictures automatically (facial recognition) without a specific legal basis (e.g. consent) for this new purpose.*[94]

86. The harms of biometric data processing are even greater and concerning for fundamental rights when considered in the context of law enforcement use. These will be further explored in section VI.A below. For the time being, PI submits that the risks are too high for a private entity to be allowed to perform mass scale and indiscriminate processing of biometric data.

(b) Chilling effect on fundamental rights

87. The Art 29 WP provides that in assessing the impact of the processing, "[t]he chilling effect on protected behaviour, such as freedom of research or free speech, that may result from continuous monitoring/tracking, must also be given due consideration."[95] PI would like to draw attention to the jurisprudence of German courts and authorities, who have conducted extensive assessments of the impact of video surveillance on fundamental rights in the context of legitimate interests assessments. In particular, the Data Protection Authority of Baden-Württemberg emphasized the importance of the right to free development of personality to assess the intensity of the monitoring through video surveillance:[96] it found that in restaurants, adventure parks and in general places where people gather to eat, drink, discuss and relax, the right to free development of personality shall override the legitimate interests of the controller. As the Internet

---

[92] OHCHR, 'The right to privacy in the digital age' (UN Doc A/HRC/39/29, 3 August 2018). Available at https://undocs.org/A/HRC/39/29.
[93] Article 29 Data Protection Working Party, 'Opinion 03/2012 on developments in biometric technologies'. Available at https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp193_en.pdf.
[94] Ibid.
[95] Art 29 WP Opinion on Legitimate Interests (n 80).
[96] Der Landesbeauftragte für den Datenschutz Baden-Württemberg, Orientierungshilfe „Videoüberwachung durch nicht-öffentliche Stellen', p. 9.

has become a socialising place on equal footing with such public spaces, the same principle ought to apply. In addition, the risks of video surveillance identified are compounded when mass real-world identification is enabled by Clearview's technology.

88. The EDPS explicitly considers SOCMINT, which is precisely the practice that Clearview's technology enables and is designed to facilitate, has considerable chilling effects on various rights and freedoms:

> *Social media users monitoring is a personal data processing activity that creates high risk for individuals' rights and freedoms. Repurposing of data is likely to affect a person's information self-determination, further reduce the control of data subjects over their data... Indeed, the diminution of intimate space available to people, as a result of unavoidable surveillance by companies and governments, has a chilling effect on people's ability and willingness to express themselves and form relationships freely, including in the civic sphere so essential to the health of democracy.*[97]

89. Further, the United Nations Human Rights Council has urged caution with regard to SOCMINT. General Comment No. 37 on Article 21 of the International Covenant on Civil and Political Rights (Right of peaceful assembly), adopted by the UN Human Rights Committee, established that:

> *The mere fact that a particular assembly takes place in public does not mean that participants' privacy cannot be violated. […] The same applies to the monitoring of social media to glean information about participation in peaceful assemblies. Independent and transparent scrutiny and oversight must be exercised over the decision to collect the personal information and data of those engaged in peaceful assemblies and over its sharing or retention*[98]

90. The Internet and social media platforms have come to play a vital role for the development of individuals' private social and political life, as well as their online identity. They constitute the digital life setting of today's civic spaces where people access information, formulate and discuss ideas, raise dissenting views, consider possible reforms, expose bias and corruption, and organise to advocate for political, economic, social, environmental, and cultural change.[99]

91. It is crucial for a healthy, striving and open Internet that individuals feel free to share personal information and photos as they see fit without fear of this personal information being immediately grabbed and stored for undisclosed purposes. The freedom to define oneself as one sees fit in different Internet fora, by controlling the distribution of different pieces of information in different places, is taken away by the looming threat of all this diverse information being traceable and unified at the click of a button.

---

[97] EDPS (n 60).
[98] Available at https://www.ohchr.org/EN/HRBodies/CCPR/Pages/GCArticle21.aspx.
[99] Privacy International, 'Protecting civic spaces' (May 2019). Available at https://privacyinternational.org/long-read/2852/protecting-civic-spaces.

(c) Harms for vulnerable communities

92. Clearview's tool can also cause particular harm to individuals in vulnerable positions. For this section we have been greatly informed by, and would like to draw attention to, the work of the American Civil Liberties Union (ACLU) in their submissions against Clearview in the state of Illinois under the BIPA.[100]

93. Individuals in vulnerable positions are at heightened risk if identified when going about their lives. Survivors of sexual harm or commercial sexual exploitation, for example, or migrants, have repeatedly been targeted for harassment or discrimination by private citizens and police officers alike. "By divesting these individuals of control over and security in their sensitive biometric identifiers and threatening to make it trivially easy to identify and track them both online and in the physical world, Clearview's system exposes them to stalking, harassment, and violence."[101] The fear of being identified may also cause these individuals to avoid attending places and meetings to access the support services they need.

94. In addition, the hashing of vectors performed when Clearview extracts biometric features from facial images potentially allows for categorisation of people's faces according to degrees of similarity. This raises the possibility for Clearview's clients to perform automatic groupings of people based on their ethnicity, colour, or other categorisation – and opens the door to discriminatory tracking and monitoring, or practices like predictive policing.

95. Having set out the multiple and serious risks and harms raised by Clearview's activities for individuals' rights and freedoms, PI submits that the balance of legitimate interests assessment must lie against the finding of a valid legal basis under Article 6(1)(f) of the UK GDPR. The lack of a legal basis under Article 6 of the UK GDPR is sufficient to find unlawful processing, but in case the ICO were minded to disagree, the next section assesses the applicability of a legal basis for special categories data processing.

<u>Manifestly made public – Article 9(2)(e) UK GDPR</u>

96. Because Clearview is processing special categories data, in addition to a valid legal basis under Article 6 (which is absent, as demonstrated in the preceding section), it must also satisfy at least one of the conditions in Article 9(2). The only relevant condition to Clearview's circumstances is that "processing relates to personal data which are manifestly made public by the data subject", under Article 9(2)(e) of the UK GDPR. PI notes that even if such condition were to apply, it would only apply to the facial images (themselves biometric data, see section V.A above) that Clearview collects online – the biometric data that Clearview creates through vector extraction cannot possibly meet this condition.

---

[100] Complaint, ACLU and others v. Clearview AI, Inc., Circuit Court of Cook County, Illinois, Case No.: 2020 CH 04353. Available at https://www.aclu.org/legal-document/aclu-v-clearview-ai-complaint.
[101] Plaintiff's response to defendant's motion to dismiss, ACLU and others v. Clearview AI, Inc., Circuit Court of Cook County, Illinois, Case No.: 2020 CH 04353.

97. Information being publicly available online is not an automatic legal basis for processing under Article 9. As authoritatively recognised by various guidance from data protection authorities and related academic commentary,[102] the exception under Article 9(2)(e) must be narrowly construed. In particular, the terms "manifestly" and "by the data subject" require very specific circumstances of the personal data having been made public.

98. First, information publicly available online must still carry a significant degree of privacy protection. This is crucial to a healthy and open Internet where individuals can exercise their fundamental rights and freedoms. Clearview's FRT tool is the archetype of a seemingly innocuous new technology that if allowed to be deployed and used at scale, could profoundly alter the Internet as we know it and individuals' behaviour online. It is operating on the flawed assumption that what is publicly available on the Internet immediately belongs to an entirely public sphere and has been benevolently offered to the whole world to see instantly and to re-use at will. But a stark divide between the public and the private spheres bears little relevance to modern societies where major parts of our economic, social and democratic lives are led online. It is misunderstanding the Internet to see it as a homogeneous, entirely public and fully accessible forum on which everyone consents to their personal information being "fair game" for all to grab as soon as it has entered a technically public part of the Internet.[103]

99. The dangers of such a stark divide are also very real in the offline world, as previously recognised by the ECtHR. As the Court held in *Peck v. UK*[104], the disclosure to the media for broadcast use of video footage of the applicant whose suicide attempt was caught on close circuit television cameras constituted a serious interference with the applicant's private life, notwithstanding that he was in a public place at the time. In that case, the ECtHR's reasoning rested on the assumption that no person could reasonably expect footage depicting sensitive aspects of their private life to be later released in the media, even if their actions are "already in the public domain".[105]

100. Second, it is common knowledge for anyone even mildly versed in using the Internet and social media that many online photos of individuals have not been made public *by the data subject* themselves. Social media allows a user to upload photos of themselves, and of any other person. These other persons (may they be friends of the uploader, unknown bystanders in public spaces, or customers of businesses that post pictures of their establishment and clients online) have not themselves uploaded their facial images online, and may not even know that photos containing their faces have been uploaded and are present on the public Internet.

---

[102] For further information and references to DPA guidance, see Edward S Dove and Jiahong Chen, 'What does it mean for a data subject to make their personal data 'manifestly public'? An analysis of UK GDPR Article 9(2)(e)' (2021) Vol. 00, No. 0, International Data Privacy Law, 1, 2. Available at https://doi.org/10.1093/idpl/ipab005.

[103] See EDPS quotation cited at paragraph 88 above, as well as UNHRC quotation cited at paragraph 89.

[104] App no 44647/98 (ECtHR, 28 January 2003), paras 53, 61-62.

[105] Ibid.

101. The OPCC reached the same conclusion when assessing whether the personal data that Clearview collects falls within the Canadian "publications" exception, which applies only "where the individual has provided the information" or where "it is reasonable to assume that the individual that the information is about provided that information": "As Clearview engages in mass collection of images through automated tools, it is inevitable that in many instances, the images would have instead been uploaded by a third party."[106]

102. Third, as explained in section III, once collected, photos are kept in Clearview's database indefinitely, with no regard for whether these photos are still publicly available at any one point. As rightly observed in a New York Times article on Clearview, "if your profile has already been scraped, it is too late. The company keeps all the images it has scraped even if they are later deleted or taken down".[107] It went on to note, "though Mr. Ton-That said the company was working on a tool that would let people request that images be removed if they had been taken down from the website of origin." As to this latter "excuse", it is first unacceptable that Clearview has deployed its technology without the existence of this tool, and second, such a tool would in any case only provide an extremely limited recourse for individuals – it would imply individuals (1) knowing in the first place that Clearview collects their facial images, (2) systematically submitting data subject access requests to know what photos have been collected by Clearview, (3) cross-checking results from these requests with what they have made available online, and (4) submitting individual requests for removal. This is entirely unreasonable and a blatant affront to individuals' right to control their online identities, preventing any effective exercise of data subject rights provided under the UK GDPR.

103. Finally, privacy settings are notoriously difficult to get right and to adjust so that the information one wants to remain within private online circles actually is and remains so. Research by PI has repeatedly shown how complex it is for individuals to adjust their settings to be privacy friendly, and that legal consent requirements are often not met.[108] "Dark patterns", as coined by the Norwegian Consumer Council, mean that data subjects are not always in control of their personal data online.[109]

104. PI therefore submits that Clearview cannot fulfil any condition for processing of special categories data under Article 9(2)(e) UK GDPR.

E. Purpose Limitation

[106] OPCC (n 4), para 66.
[107] Hill (n 6).
[108] Privacy International, 'Most cookie banners are annoying and deceptive. This is not consent.' (21 May 2019). Available at https://privacyinternational.org/explainer/2975/most-cookie-banners-are-annoying-and-deceptive-not-consent. Privacy International, 'Facebook - Profile Settings' (7 January 2021). Available at https://privacyinternational.org/guide-step/3959/facebook-profile-settings.
[109] Norwegian Consumer Council, 'Deceived by Design – How tech companies use dark patterns to discourage us from exercising our rights to privacy' (27 June 2018). Available at https://fil.forbrukerradet.no/wp-content/uploads/2018/06/2018-06-27-deceived-by-design-final.pdf.

105. Another core principle of data protection overtly trampled by Clearview's processing is that of purpose limitation, under Article 5(1)(b) of the UK GDPR. Application of the principle ought to consider factors listed in Article 6(4), which in this case clearly indicate that Clearview's processing is not compatible with the purpose for which the personal data was initially disclosed.

106. The question of purpose limitation is intrinsically linked to what one can expect to be done with their publicly available personal data, as explored in paragraphs 58 to 68 above. Indeed, every "making public" occurs for a specific purpose. The making public of a resume with contact data on one's own website is for the purposes of finding a job – a controller would clearly disregard the original purpose if they were to use the data for advertising purposes.

107. PI has demonstrated that re-use for processing in a biometric database clearly falls outside of such expectations. As stated by the EDPS, uses of personal data in the context of social media monitoring *"*often result in personal data being used beyond their initial purpose, their initial context and in ways the individual could not reasonably anticipate."[110]

108. The following statement in the Art 29 WP's opinion on biometrics is also telling:

> *Photographs on the internet, in social media, in online photo management or sharing applications may not be further processed in order to extract biometric templates or enrol them into a biometric system to recognise the persons on the pictures automatically (facial recognition) without a specific legal basis (e.g. consent) for this new purpose. If there is a legal basis for this secondary purpose the processing must also be adequate, relevant and not excessive in relation to that purpose. If a data subject has consented that photographs where he appears may be processed to automatically tag him in an online photo album with a facial recognition algorithm, this processing has to be achieved in a data protection friendly way: biometric data not needed anymore after the tagging of the images with the name, nickname or any other text specified by the data subject must be deleted. The creation of a permanent biometric database is a priori not necessary for this purpose.*[111]

109. In light of this statement, Clearview's processing constitutes an entirely new purpose from original publication, for which it ought to have a separate, valid legal basis. As demonstrated in section V.D above, this is inexistent, and Clearview therefore violates the purpose limitation principle.

110. PI concludes that Clearview's practices constitute breaches of the transparency, fairness and purpose limitation principles, and of the requirement for a lawful basis. PI will not seek to assess the compliance with UK GDPR of Clearview's clients' use of the tool other than that by law enforcement authorities, as these

[110] EDPS (n 60).
[111] Art 29 WP (n 93), p.7.

are the only clients that Clearview today openly markets to. We would however like to draw the attention of the ICO to reported predictions by "police officers and Clearview investors" that the tool "will eventually be available to the public".[112]

VI. Legal Framework and Concerns: Processing by Law Enforcement Authorities (Part 3 DPA 2018)

111. Restrictions to the fundamental rights of individuals are to be done by legislative measures on matters of such importance as state security, defence, prevention, investigation, detection or prosecution of criminal offences, etc.[113] While such limited restrictions can apply to processing by law enforcement authorities, through the DPA 2018, in no way can they apply to a commercial entity indiscriminately collecting personal data, with the potential ultimate purpose of selling the use of such database to strictly regulated authorities. As repeatedly observed by PI in its work,[114] the use of private tools for enforcement of the law often leads to bypassing the exacting safeguards for fundamental rights placed on public authorities.

112. While PI considers that the breaches of UK GDPR identified in section V are sufficient to warrant an order against the collection of UK data subjects' personal data by Clearview, these breaches become all the more salient when considered in conjunction with the ultimate intended use of the personal data collected and processed by Clearview. If the ICO is minded to allow Clearview's collection practices in the UK, PI submits that to limit the harm caused to data subjects, the use of such collected personal data by law enforcement authorities ought to be prohibited. It raises serious concerns and breaches of the DPA 2018.

113. This section of the submission first sets out PI's concerns with law enforcement's use of FRT and SOCMINT, concerns compounded when these technologies are used together, as in the case of Clearview. It will then identify how such concerns translate to various breaches of the DPA 2018, in particular of the first data protection principle (s.35) and its requirement of lawfulness.

A. Concerns over police use of FRT and SOCMINT

114. The use of FRT by the police has a profound impact on the way our society is monitored and policed. The roll out of such intrusive technology does not only pose significant privacy and data protection questions, but also ethical questions around whether modern democracies should ever permit its use. With Clearview's tool in hand, the police can effectively identify every single person caught on camera (or at least associate their physical identity with their online presence). A police force could very realistically decide to identify every single

[112] Hill (n 6).
[113] UK GDPR Article 23.
[114] See for example: Privacy International, 'Public-Private surveillance partnerships'. Available at https://privacyinternational.org/campaigns/unmasking-policing-inc; Privacy International, 'One Ring to watch them all' (25 June 2020). Available at https://privacyinternational.org/long-read/3971/one-ring-watch-them-all.

individual in a protest crowd and build profiles on them from information gleaned online. This is an entirely dystopian prospect that finds very realistic potential in Clearview's tool.

115. In *Bridges*, the UK High Court considered that the use of FRT by the police

> *goes much further than the simple taking of a photograph. The digital information that comprises the image is analysed and the biometric facial data is extracted. That information is then further processed when it is compared to the watchlist information. The fact that this happens when the Claimant is in a public space is not a sufficient response.*[115]

By analogy with Clearview's collection of photos from publicly available sources, the fact that these photos are public is not a sufficient response. What's more, individuals whose photos are collected by Clearview may not even be aware that their face is available on the public Internet (if those photos were uploaded by a third party).

116. FRT as deployed in public spaces for the purposes of policing does not only interfere with individuals' privacy and data protection rights, it can also seriously affect the exercise of rights to freedom of thought, conscience and religion, freedom of expression and freedom of assembly and association. The EDPS has highlighted that the use of FRT "is fundamentally an ethical question for a democratic society", since it can "obviously chill individual freedom of expression and association".[116]

117. In its submission on Article 21 of the International Covenant on Civil and Political Rights to the UN Human Rights Committee, PI highlighted how new surveillance technologies can affect the exercise of the right to freedom of peaceful assembly, by having "a chilling effect on individuals".[117] This was confirmed in General Comment No. 37: "While surveillance technologies can be used to detect threats of violence and thus to protect the public, they can also infringe on the right to privacy and other rights of participants and bystanders and have a chilling effect."[118] Due to this chilling effect, it is extremely difficult or impossible for authorities wishing to make use of these technologies to precisely measure the negative effects for the exercise of the aforementioned rights, and to thus justify its use.[119] In this regard, the United Nations High Commissioner for Human Rights has recommended that states never use FRT "to identify those peacefully participating in an assembly".[120]

---

[115] *R (Bridges) v Chief Constable of South Wales Police* [2019] EWHC 2341, para 54.
[116] EDPS, 'Facial Recognition: A solution in search of a problem?' (28 October 2019). Available at https://edps.europa.eu/press-publications/press-news/blog/facial-recognition-solution-search-problem_en.
[117] Privacy International, 'Submission on Article 21 of the International Covenant on Civil and Political Rights' (February 2019), p. 10. Available at https://privacyinternational.org/sites/default/files/2019-03/Submission%20on%20Article%2021%20of%20ICCPR_0.pdf.
[118] UN Human Rights Committee (n 98), para 10.
[119] Privacy International, 'Protecting Civic Spaces' (1 May 2019). Available at https://privacyinternational.org/long-read/2852/protecting-civic-spaces.
[120] OHCHR (n 91), para 54(h).

118. In addition to FRT, Clearview's tool enables the conduct of "overt" SOCMINT. The Office of Surveillance Commissioners (now Investigatory Powers Commissioner)' Guidance defines overt SOCMINT as looking at "open source" data, being publicly available data and data where privacy settings are available but not applied.[121] In the UK, only "covert" SOCMINT is subject to the Regulation of Investigatory Powers Act 2000 ("**RIPA**"). RIPA requires that when public authorities need to use covert techniques (such as covert social media intelligence) to obtain private information about someone, they do it in a way that is necessary, proportionate, and compatible with human rights. It also provides for the need to obtain judicial approval prior to using covert techniques and requires internal approval of a RIPA Authorising Officer as well as that of a magistrate.[122]

119. No equivalent legislation exists for the use of "overt" SOCMINT. Section 26(9)(a) RIPA provides that surveillance is covert if it is carried out in a manner that is calculated to ensure that persons who are subject to the surveillance are unaware that it is or may be taking place. This could potentially apply to overt social media monitoring, since individuals are often unaware that they are being monitored, but as things stand authorities have not considered themselves bound by RIPA when conducting overt social media monitoring.

120. PI is concerned that the safeguards designed specifically to govern the use of "overtly" collected intelligence are often lacking. There is no requirement to obtain prior authorisation when conducting "overt" social media monitoring by public authorities and law enforcement agencies, unlike for "covert" SOCMINT under RIPA.[123] This has led to a situation where law enforcement officials (and intelligence agencies) may believe that everything that a given social networking website sets as publicly available is fair game for them to access, collect, and process with very limited regulation, oversight, or safeguards.[124]

121. Social media monitoring poses significant risks for individuals' fundamental rights. Regulators and UN bodies have highlighted the need for such conduct to adhere to strict safeguards. In its case law, the ECtHR has emphasised that "domestic law must afford appropriate safeguards to prevent any such use of personal data as may be inconsistent with the guarantees of" Article 8 of the Convention.[125] These safeguards need to govern all processing operations performed on personal data by public authorities, including their collection, retention or storage, analysis, dissemination or disclosure, or any other form of processing. As the Court highlighted in *Marper*:

---

[121] Privacy International, Office of Surveillance Commissioners Guidance - Covert surveillance of Social Networking Sites (SNS), 24 May 2020. Available at https://privacyinternational.org/long-read/3537/office-surveillance-commissioners-guidance-covert-surveillance-social-networking.
[122] UK Home Office, 'Surveillance and counter-terrorism guidance' (26 March 2013). Available at https://www.gov.uk/guidance/surveillance-and-counter-terrorism.
[123] Ibid, p. 10.
[124] Ibid, p. 17.
[125] *S. and Marper v. UK* [GC], App nos 30562/04 and 30566/0 (ECtHR, 12 April 2008), para 103.

The need for such safeguards is all the greater where the protection of personal data undergoing automatic processing is concerned, not least when such data are used for police purposes. The domestic law should notably ensure that such data are relevant and not excessive in relation to the purposes for which they are stored; and preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored […]. The domestic law must also afford adequate guarantees that retained personal data were efficiently protected from misuse and abuse […]. The above considerations are especially valid as regards the protection of special categories of more sensitive data.[126]

122. Overall, bulk monitoring can interfere with people's rights to express themselves anonymously, formulate and share their thoughts, engage in controversial dialogue, attend public gatherings, and seek redress of grievances against the government. In the long-term, this may lead to self-censorship: people may avoid visiting certain social media profiles, liking, sharing, re-tweeting controversial posts, joining certain discussion groups, or even using certain words. Ultimately, this self-censorship can change how people seek out new information, develop and discuss ideas, and organise around them.[127]

123. In addition, the routine collection and processing of publicly available information for intelligence gathering may lead to the kind of abuses we observe in other forms of covert surveillance or other police operations. This can involve the systematic targeting of certain ethnic and religious groups by law enforcement agencies. It is impossible to guarantee that there is no racial or religious bias in online monitoring if there is no notice, transparency and oversight. And as law enforcement agencies are often secretive about the use of social media monitoring and sources of information, it can be extremely difficult for individuals to challenge any potential unlawful use of such data.[128]

124. Any processing operation performed by authorities upon individuals' personal data published on social media for purposes that goes beyond what individuals might expect or foresee should be regarded as a serious interference with their right to respect for private life, particularly when such processing involves the use of FRT to connect and compound the sources of information. To hold otherwise would be to deny the necessary protection afforded by the ECHR to individuals' private life in the digital environment, a field "where abuse is potentially so easy in individual cases and could have such harmful consequences for democratic society as a whole".[129]

B. Breach of First Data Protection Principle: Lawfulness

[126] Ibid.
[127] Privacy International, 'Protecting Civic Spaces' (n 119).
[128] Privacy International, 'Is your Local Authority looking at your Facebook likes?' (May 2020), p. 7. Available at https://privacyinternational.org/sites/default/files/2020-05/Is%20Your%20Local%20Authority%20Looking%20at%20your%20Facebook%20Likes_%20May2020.pdf.
[129] *Klass v. Germany*, App no 5029/71 (ECtHR, 6 September 1978), para 56.

125. Under s.35(2) of the DPA 2018, processing of personal data for a law enforcement purpose is lawful only to the extent that it is "based on law" and either the data subject has given consent to the processing for that purpose (which cannot apply here), or the processing is necessary for the performance of a task carried out for that purpose by a law enforcement authority. In addition, in the case of sensitive processing, processing is only permitted where it is strictly necessary for the law enforcement purpose, meets at least one of the conditions in Schedule 8, and the controller has an appropriate policy document in place at the time when the processing is carried out (s.35(3) and (5) DPA 2018).

126. The ICO published in 2019 an opinion on the use of live facial recognition ("**LFR**") by law enforcement,[130] finding that such use constitutes sensitive processing under s.35(8)(b) DPA 2018. In particular, the ICO noted that this applies "in respect of **all** facial images captured and analysed by LFR software, irrespective of whether that image yields a possible match to a person on a watchlist; or the biometric data of unmatched persons is deleted within a short period of time". The use of Clearview's FRT tool is the online equivalent of LFR – leaving images of oneself on publicly available parts of the Internet is very similar in process as exposing oneself in physical public spaces. It is even more unwillingly expository, as individuals may not be aware of the presence of their images online, and those online images are very often linked to other information such as name, profession, relational network, etc.

127. Clearview's tool can also be compared with Automated Facial Recognition ("**AFR**") as assessed in the UK Court of Appeal case of *Bridges*,[131] as its technical stages are the same as described in the Court's judgment in paragraph 9. A crucial difference, though, makes Clearview's technology a tool of mass surveillance that is invasive of privacy on a much larger scale: because everyone is liable to be included in Clearview's database, it effectively puts everyone, indiscriminately, on a watchlist.

128. PI therefore submits that any findings in relation to the use of LFR and AFR and minimum thresholds for its use ought to apply to the use of Clearview's FRT tool. PI also submits that owing to the nature of Clearview's tool as described throughout this submission and characterised by systematic and indiscriminate collection, processing as biometric data, and indefinite retention, any existing conditions and safeguards for the use of LFR and AFR simply cannot be met to authorise the use of Clearview's tool.

129. This part of the submission will now set out why any use of Clearview's tool by law enforcement authorities cannot meet the requirements of s.35 of the DPA 2018, as it is:

---

[130] Information Commissioner's Office, 'The use of live facial recognition technology by law enforcement in public places' (Information Commissioner's Opinion, 2019/01, 31 October 2019). Available at https://ico.org.uk/media/about-the-ico/documents/2616184/live-frt-law-enforcement-opinion-20191031.pdf.

[131] *R (Bridges) v Chief Constable of South Wales Police* [2019] EWHC 234.

(a) Not based on law – s.35(1); and
(b) Not strictly necessary – s.35(5)(a).

Not based on law

130. The lack of sufficient legal framework for the use of AFR technology by the police was made very clear in the case of *Bridges*, which found profound deficiencies in that legal framework. In that case, a crucial question relevant to whether use of the technology was based on law was the "who" question, i.e. whether relevant laws or policies give adequate guidance as to who can be put on an AFR watchlist in the first place. The relevant policy required that watchlists be "proportionate and necessary", and for this required consideration of the number, quality and provenance of images, and rationale for their inclusion. It also provided some broad categories of individuals who could be placed on the watchlist. The Court found that this policy did not appropriately govern the "who" question, and therefore that the legal framework for the use of the technology was not sufficient.[132]

131. Applying that analysis to Clearview's tool, the "who" question is easily answered – everyone who has at least one facial image of themselves online will be put on the watchlist. Any such indiscriminate watchlist policy is clearly unacceptable in light of the Surveillance Camera Commissioner ("**SCC**")'s guidance on FRT watchlists,[133] and in light of common sense and expectations in a modern democracy.

132. The Surveillance Camera Code of Practice issued by the Secretary of State for the Home Department in June 2013 (the "**SC Code**")[134] is the closest relevant guidance to the use of Clearview's tool, as the latter is a system "for […] processing or checking images or information obtained by systems [for recording or viewing visual images for surveillance purposes]", as defined in section 29 of the Protection of Freedoms Act 2012. The following provisions of the SC Code demonstrate that a tool like Clearview's simply cannot be deployed under the current legal framework:

(a) "2.4 The decision to use any surveillance camera technology must, therefore, be consistent with a legitimate aim and a pressing need. Such a legitimate aim and pressing need must be articulated clearly and documented as the stated purpose for any deployment. The technical design solution for such a deployment should be proportionate to the stated purpose rather than driven by the availability of funding or technological innovation." – a pressing need

[132] *R (Bridges) v Chief Constable of South Wales Police* [2019] EWHC 234, paras 128-129.
[133] Surveillance Camera Commissioner, 'Facing the Camera – Good Practice and Guidance for the Police Use of Overt Surveillance Camera Systems Incorporating Facial Recognition Technology to Locate Persons on a Watchlist, in Public Places in England & Wales' (November 2020), paras 4.20-4.25. Available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/940386/6.7024_SCC_Facial_recognition_report_v3_WEB.pdf.
[134] Home Office, 'Surveillance Camera Code of Practice' (June 2013). Available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/282774/SurveillanceCameraCodePractice.pdf.

for using Clearview's product is difficult to identify, given the inherent uncertainty of success in identifying a suspect through online information. Rationale for the use of Clearview's product would fall squarely into what the SC Code calls "availability of technological innovation". Any identified purpose would in any case be disproportionate to the indiscriminate collection and extraction of biometric information from everyone's facial images.

(b) "3.2.3 Any use of facial recognition or other biometric characteristic recognition systems needs to be clearly justified and proportionate in meeting the stated purpose, and be suitably validated[4]. [footnote 4: The Surveillance Camera Commissioner will be a source of advice on validation of such systems.]" – any individual deployment or use of Clearview's would need to be reviewed and validated by the SCC. This goes against any general deployment of Clearview in a police unit, defeating any speculative usefulness of a technology that works as a shot in the dark.

133. Related to the requirement of law, any use of Clearview's tool by the police would require having a specific policy in place that justifies its legitimacy and specificity, through what the SCC guidance referred to as the "5WH" question (What, Who, Why, Where, When and How). In the context of technologies such as ANPR or facial recognition systems, the SC Code requires system operators to have "a clear policy to determine the inclusion of […] a known individual's details on the reference database associated with such technology". Any such policy would simply not work for Clearview's tool, which systematically and indiscriminately collects photos and personal details from all individuals and produces biometric identifiers on every single one of them.

134. Finally, as explained above in section VI.A, the conduct of "overt" SOCMINT is not currently governed by any law. For all these reasons, the use of Clearview's tool by law enforcement authorities cannot be considered to be based on law, let alone a law that is clear, precise and foreseeable in its application.

Not strictly necessary

135. Necessity requires the police to prove a concrete, specific and immediate threat to national security or public safety that would justify the need for deploying this kind of technology. The ECtHR has applied a test of strict necessity to interferences with the right to privacy in the surveillance context. In *Szabó and Vissy v. Hungary*, the ECtHR indicated that given "the potential of cutting-edge surveillance technologies to invade citizens' privacy,"

> *[a] measure of secret surveillance can be found as being in compliance with the Convention only if it is strictly necessary, as a general consideration, for the safeguarding [of] democratic institutions and, moreover, if it is strictly necessary, as a particular consideration, for the obtaining of vital intelligence in an individual operation. In the Court's view, any measure of secret surveillance which does not correspond to these criteria will be prone to abuse by the authorities with formidable technologies at their disposal. The*

Court notes that both the Court of Justice of the European Union and the United Nations Special Rapporteur require secret surveillance measures to answer to strict necessity – an approach it considers convenient to endorse.[135]

136. The ICO provides that strict necessity in the context of sensitive processing of personal data through LFR by law enforcement requires the controller to "consider the proportionality of the sensitive processing and the availability of viable alternatives to LFR".[136] PI submits that Clearview's tool could never be found to be strictly necessary, because using it constitutes a complete shot in the dark – the police could never be confident that using it would be even likely to produce a positive match, as opposed to when using "traditional" defined watchlists that exclusively contain reasonable suspects.

137. In the context of data retention measures, the CJEU has held that in order to be limited to what is strictly necessary, these measures must be subject to restrictions which "circumscribe, in practice, the extent of that measure and, thus, the public affected".[137] The public affected, in Clearview's case, is effectively the entire population – thereby putting everyone on a watchlist. Despite the fact that the retention of data in Clearview's case is done by a private company rather than by the police, the same test ought to apply: the harms identified by courts and authorities in indiscriminate and indefinite retention remain the same when law enforcement authorities are given blanket access to Clearview's database. PI urges the ICO to prevent evasion by public authorities of their human rights and data protection law obligations by preventing reliance on a private tool for their surveillance operations without holding that tool to the same obligations.

138. In addition, the indiscriminate collection, storage and processing of photos by Clearview can easily be compared to any bulk collection of data, which has been considered unlawful.[138] The risk of abuse of bulk datasets is considerable, which is why the CJEU found that "general access to all retained data, regardless of whether there is any link, at least indirect, with the aim pursued, cannot be regarded as being limited to what is strictly necessary"[139].

139. As part of a necessity assessment, the principle of proportionality ought to be taken into account – necessity is actually subject to proportionality, per the EDPS' toolkit on assessing necessity, so that only a strictly necessary measure ought should proceed to the proportionality test.[140] In *S. and Marper v. UK*,[141] the ECtHR dealt with another measure involving the indiscriminate retention of

---

[135] App no 37138/14 (ECtHR, 13 October 2015), para 73.
[136] ICO (n 130) p. 14.
[137] Joined Cases C–203/15 and C–698/15 *Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson* [2016] ECR I–970, para 110.
[138] Case C-623/17 *Privacy International v SSFCA and Ors* [2020] ECLI:EU:C:2020:790.
[139] Ibid, para 78.
[140] EDPS, 'Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit" (11 April 2017), p. 5. Available at https://edps.europa.eu/sites/edp/files/publication/17-06-01_necessity_toolkit_final_en.pdf.
[141] App nos 30562/04 and 30566/04 (ECtHR, 12 April 2008).

biometrics, i.e. fingerprints, DNA and cellular samples, for the purposes of detecting and prosecuting crime. It observed:

> *the protection afforded by Article 8 of the Convention would be unacceptably weakened if the use of modern scientific techniques in the criminal-justice system were allowed at any cost and without carefully balancing the potential benefits of the extensive use of such techniques against important private-life interests. In the Court's view, the strong consensus existing among the Contracting States in this respect is of considerable importance and narrows the margin of appreciation left to the respondent State in the assessment of the permissible limits of the interference with private life in this sphere. The Court considers that any State claiming a pioneer role in the development of new technologies bears special responsibility for striking the right balance in this regard.*[142]

140. The concerns set out in section VI.A above demonstrate the serious interference with privacy, data protection and other fundamental rights that Clearview's tool constitutes. This serious interference weighs heavily in the balance against any potential benefits of the technology. In addition, in the context of FRT, any balancing between the benefits of this surveillance technology and the human rights harms will be very difficult given the challenges of adequately incorporating the extent of the latter due to FRT's chilling effects. For example, authorities would likely not be in a position to assess the exact number of people who have chosen not to attend a public event, sacrificing their freedom of expression and assembly rights over legitimate concerns relating to abuse of their biometric data by the police. Given the bulk and indiscriminate nature of the data collected and processed by Clearview, and the serious human rights concerns raised by its use to facilitate the deployment FRT, PI submits that law enforcement use of Clearview can never be proportionate.

VII. Applications / Remedy

141. For the reasons above, PI welcomes the ICO's decision to open an investigation into Clearview jointly with the Australian Information Commissioner,[143] and respectfully requests that the ICO take the concerns expressed in this submission into account as part of those investigations.

142. In summary, PI invites the Commissioner to consider:

(a) Clearview's initial collection of images and processing of biometric data, in that respect:
   i. The transparency and fairness principles, in particular with reference to data subjects' reasonable expectations of privacy;

[142] Ibid, para 112.
[143] ICO (n 12).

ii. The requirement for a lawful basis under both Articles 6 and 9 of the UK GDPR, in particular whether reliance on the "legitimate interests" and "manifestly made public" bases is justified;
iii. The purpose limitation principle;

(b) The use of Clearview's tool by law enforcement authorities, in that respect the lawfulness of such processing, with regard in particular to the risks of harm to data subjects' fundamental rights and freedoms.

143. PI requests that the ICO issue an enforcement notice requiring Clearview to stop all collection and processing operations on personal data of data subjects in the UK, under Article 58(2)(f) of the UK GDPR.

144. In addition, PI requests that the ICO issue an assessment notice of the use of Clearview's tool by police forces in the UK, under s.146 of the DPA 2018.

145. As set out in this submission, Clearview's data collection and processing activities know no borders, potentially extending to individuals in any country around the world. Therefore, PI invites the ICO to coordinate its enforcement action with other supervisory authorities in the EU, who have received similar complaints from PI and other civil society organisations.

Privacy International

27 May 2021