IN THE UPPER TRIBUNAL **Appeal No. UA-2024-001563-**
GIA (ADMINISTRATIVE APPEALS CHAMBER)

ON APPEAL FROM THE FIRST-TIER TRIBUNAL
(GENERAL REGULATORY CHAMBER)
[2023] UKFTT 819 (GRC) ("Judgment")

B E T W E E N:

THE INFORMATION COMMISSIONER

Appellant

-and-

CLEARVIEW AI INC

Respondent

-and-

PRIVACY INTERNATIONAL

Intervener

INTERVENER'S SKELETON ARGUMENT FOR HEARING 9-11 JUNE 2025

---

*References to the Information Commissioner's Skeleton Argument are in the form ICO Skel §**

*References to Clearview's Response to the Grounds are in the form Response §**

*References to pages of the First-Tier Tribunal Bundle, Upper Tribunal and Additional Bundle are respectively in the form **[FTTB/*]**, **[UTB/*]** and **[AB/*]***

A INTRODUCTION AND SUMMARY

1. Privacy International is a charity that defends the right to privacy around the world. It has litigated both domestically and internationally to protect privacy rights against incursions from surveillance technology and, in particular, made detailed submissions about the Respondent's ("**Clearview's**") technology to a number of data protection authorities.

2. Privacy International is grateful for the Tribunal's permission to intervene in these proceedings. As far as possible, the submissions below seek to avoid repeating arguments that have already been addressed in the skeleton argument of the Information Commissioner dated 14 May 2025. In particular, given the indications of the Information

Commissioner and the Tribunal,[1] the arguments below focus on: (i) an international perspective which explains the unjustifiable divergence between the UK and the EU (and other jurisdictions) as a result of the Judgment; and (ii) the technical and principled reasons why Clearview's technology amounts to a form of mass surveillance.

3. For the reasons set out in more detail below, Privacy International makes the following submissions in support of the appeal:

   (1) **Extra-territoriality and state immunity (Grounds 1-2).** The question under Art. 3(2A) UK GDPR is the same as that under Art. 2(2)(a) EU GDPR. It is well-established that Art. 2(2)(a) EU GDPR is a narrow exception which exempts national security processing by EU Member States. It does not apply to third country states, much less private actors contracted by third country states. The First Tier Tribunal erred in creating a zone of immunity for the benefit of a private actor, and thus leaving persons in the UK in a materially worse position than their counterparts in the EU. These points are developed in **Section D.1** below.

   (2) **"Monitoring behaviour" (Additional Reasons).**[2] The First Tier Tribunal was clearly correct to conclude that Clearview's processing related to monitoring behaviour in the UK. At least five other EU regulators independently reached the same result in respect of the identical provision in the EU GDPR. As Privacy International has analysed and publicly explained in recent years, each part of Clearview's processing activities is highly intrusive and its technology cannot be characterised as a mere storage database or search engine. This point is developed in **Section D.2** below.

4. Before turning to these arguments, this skeleton argument summarises the submissions, of relevance to this appeal, that have been made by Privacy International to EU regulators about Clearview (**Section B**) as well as key aspects of the legal framework which have not yet been addressed in detail by the principal parties (**Section C**).

---

[1] Information Commissioner's Response to Privacy International's application to intervene at §7 **[UTB/276]** and the Upper Tribunal's Order granting permission to intervene dated 19 May 2025 at §§11 and 14(a) **[UTB/271]**.

[2] Privacy International understands from the Order of the Tribunal §14(a) **[UTB/271]** that the Tribunal would be assisted by submissions on these points.

B PRIVACY INTERNATIONAL'S INTEREST IN THIS APPEAL

5. Privacy International's general expertise and experience were set out in its application to intervene and are not repeated here.[3] Its profound concern about Clearview's technology has been the subject of submissions to regulatory authorities as set out below.

B.1 Complaint to the Information Commissioner

6. On 27 May 2021, Privacy International submitted a complaint against Clearview to the Information Commissioner's Office.[4] The complaint ("**PI Complaint**") addressed the following matters which are relevant on this appeal:

   (1) First, Privacy International provided an explanation of the functionality of Clearview's technology (§§4-7) **[AB/395-397]**. This technical overview informed its submissions that Clearview's facial recognition technology was particularly invasive (§§39-43, 114-124) **[AB/405-406, 427-430]**. Privacy International specifically responded to Clearview's arguments (still maintained on this appeal) that the relevant data was already public and that Clearview simply operates a "search engine" (§§56, 59-62, 97-102) **[AB/409-410, 424-425]**.

   (2) Second, Privacy International put forward case studies involving data subject access requests made by two Privacy International employees in the UK in April 2020.[5] Clearview's responses revealed that the employees' images (and in one case, name) were held by Clearview, including: (i) three photos and descriptions of one employee and (ii) eight photos and descriptions of another (§22). In the latter case, one photo was incorrect because it was a photo of an unknown individual (§22) **[AB/401]**.

   (3) Third, Privacy International drew attention to the "real-life" privacy harms associated with this technology, including chilling effects on participation in democratic processes, constraints on the development of their socio-political

---

[3] Privacy International's application to intervene §§8-12 **[UTB/241-242]**.

[4] Privacy International, 'Submission to the Information Commissioner – Request for assessment of processing operations by Clearview AI, Inc.' (27 May 2021), available online. **[AB/395]** An identical complaint was filed in French to the national regulator in France: Privacy International, 'Réclamation auprès de la Commission Nationale De L'informatique et des Libertés' (27 mai 2021), available online.

[5] At that time, Clearview's privacy policy stated that residents of the European Economic Area or of Switzerland could exercise their rights under the GDPR, and linked to a "EU/UK/Switzerland Data Access Form" and "EU/UK/Switzerland/Australia Opt-Out" form. This privacy policy was replaced in March 2021 by a version that removed this reference. See PI Complaint §27 **[AB/402]**.

identities, and vulnerability to stalking and self-censorship (§§33, 51-57, 76, 92-94) **[AB/33, 407-409, 414, 423]**.

(4) Fourth, Privacy International recounted global regulatory developments demonstrating widespread concern about the scope and impact of Clearview's technology (§§8-14) **[AB/397-399]**. The complaint referred to regulatory action in Germany, the Netherlands, Canada and Australia and litigation in Illinois (§§24-25, 31, 79 and 92) **[AB/401, 403, 419-423]**.

(5) Fifth, Privacy International made submissions about the application of the UK GDPR. It was explained that Clearview was within the scope of Article 3(2)(b) of the UK GDPR since it "*engaged in monitoring of the behaviour of data subjects within the UK*" (§15) **[AB/399]**. It was also submitted that there was no reason that the ICO "*should reach a different conclusion*" from the EU regulators because the applicability of the UK GDPR "*follows the same principles as the EU GDPR*" (§26) **[AB/401]**.

7. In short, the PI Complaint alleged that Clearview's processing, and the use of its technology by public and private sector clients, had been evading all the safeguards for surveillance technologies developed by UK and European Courts over the years. Those submissions are of direct relevance to this appeal and they are developed further below in respect of the specific issues arising on this appeal in **Section D** below.

B.2 Complaints to EU Regulators

8. In the period since the PI Complaint, at least five EU regulators have issued enforcement notices against Clearview under the EU GDPR. Privacy International was involved in assisting with complaints in Italy, France, Greece and Austria in particular.[6]

9. These decisions are significant because they show a remarkably consistent approach to jurisdiction under the EU GDPR. While each regulator acknowledged that Clearview was domiciled in the US, Article 3(2)(b) of the EU GDPR ("*monitoring behaviour*") was relied upon to bring Clearview's activities in scope. Furthermore, it is telling that none of the regulators had any hesitation in regarding Clearview as being within their enforcement

[6] See 'Challenge against Clearview AI in Europe', available online, which compiles the action taken in respect of Clearview across several jurisdictions.

remit despite Article 2(2)(a) of the EU GDPR (equivalently Article 3(2A) in the UK GDPR) and despite the general principle of state immunity in international law.

(i) Italy

10. On 10 February 2022, the Italian data protection authority ("**GPDP**") issued an enforcement order against Clearview pursuant the EU GDPR.[7]

11. At that time, Clearview had argued that the Italian regulator had no jurisdiction, on the basis that it did not carry out monitoring under Article 3(2)(b). It was argued that "*the concept of monitoring implies continuous and persistent observation*" whereas Clearview's "*product is an image search application that provides search results with links to third-party websites*" (§2) **[FTTB/1204]**. The GPDP rejected these submissions. Given the sophisticated methods used by Clearview – to scrape images, extract facial recognition data, conduct identification, and match to other personal information – it went far beyond an ordinary search engine (§3.1) **[FTTB/1213]**.

12. The Italian regulator went on to find several breaches of the EU GDPR, which it regarded as very serious, and issued an injunction and a monetary penalty of €20m (§3.6) **[FTTB/1226]**.

(ii) Greece

13. On 13 July 2022, the Greek data protection authority ("**HDPA**") issued an enforcement notice against Clearview.[8]

14. As above, Clearview had argued that the HDPA had no jurisdiction over it as a US-based entity **[AB/439]**. Nonetheless, the Greek regulator applied Article 3(2)(b) and found that Clearview was engaged in processing relating to "*monitoring behaviour*" (§12) **[AB/451]**. It was noted that the "*analysis*" of information that "*a person chooses to publish on the internet … allows the determination of that person's behaviour*" **[AB/451]**.

---

[7] Garante per la Protezione dei Dati Personali 'Ordinanza ingiunzione nei confronti di Clearview AI - 10 febbraio 2022 [9751362]', available online. **[FTTB/1201]**

[8] Hellenic Data Protection Auhthority, 'Επιβολή προστίμου στην εταιρεία Clearview AI, Inc', available online. **[AB/437]**

15. The regulator found several breaches of the EU GDPR and issued a mandatory order to comply with the legislation (pp. 20-21) **[AB/456-457]**. It subsequently imposed a €20 million penalty.

(iii) France

16. On 17 October 2022, the French data protection authority ("**CNIL**") issued an enforcement notice against Clearview.[9]

17. This followed Privacy International's complaint to the CNIL which included the same content as set out in the PI Complaint to the Information Commissioner. As far as the French investigation is concerned, Clearview made no submissions and did not appear to engage with the process.

18. After setting out the legal principles, the CNIL concluded that Clearview's processing was "*related to the monitoring of behaviour*" under Article 3(2)(b) of the EU GDPR including because it involved using several pieces of information to build a behavioural profile. This was at least "*linked to*" monitoring (§§27-41).

19. The CNIL found various breaches of the EU GDPR, noting that the processing is "*particularly intrusive*" and that "*the vast majority of the data subjects are unaware of its existence*" (§§64-65). An enforcement notice and fine of €20 million were issued against Clearview (§107). There was also an injunction with a daily penalty (§112).

(iv) Austria

20. On 9 May 2023, the Austrian data protection authority ("**DSB**") issued a decision finding unlawful conduct against Clearview and ordering deletion of data (but issuing no penalty).[10]

21. Clearview had objected to the jurisdiction of the DSB along similar lines as it objects in these proceedings. However, the DSB concluded that Article 3(2)(b) of the EU GDPR was satisfied. It was noted that "*related to*" had a broad meaning and that "*the aim of the EU legislator was to provide data subjects in the EU with comprehensive protection against their behaviour being monitored by controllers not established in the EU*" (p. 14)

---

[9] Commission Nationale de l'informatique et des Libertés, 'Restricted Committee Deliberation No. SAN-2022-019 of 17 October 2022 concerning CLEARVIEW AI', available online [This decision is not in the bundle but the earlier decision dated 1 November 2021 reaching the same view is at [**FTTB/1243**]].

[10] Österreichische Datenschutzbehörde, 'Bescheid', available online. **[AB/458]**

[AB/471]. It was explained that Clearview's technology met the threshold of monitoring behaviour because "*it is possible to gather a lot of different information about a person and find out more about their personal preferences, behaviour or habits*" (p. 15) **[AB/472]**.

(v) Netherlands

22. On 16 May 2024, the Dutch data protection authority ("**AP**") issued a penalty notice against Clearview for "*serious violations*" of the EU GDPR.[11]

23. Again, Clearview had disputed jurisdiction. In a sophisticated and lengthy decision, the AP considered that Clearview's activities were covered by the extra-territorial scope established by Article 3(2)(b) of the EU GDPR. It was explained for instance that Clearview's clients were able to learn about individuals in the photos over time including to predict their behaviour (§§64-65) **[AB/500]**.

24. The AP also specifically rejected the argument as to national security under Article 2(2) of the EU GDPR as follows:

> "23. The exceptions to the applicability of the GDPR as listed in Article 2(2) GDPR, according to the Court of Justice of the European Union (hereinafter: CJEU) should be interpreted strictly.
>
> 24. In that connection the CJEU considered that Article 2(2), opening words and subsection (a) GDPR, read in the light of recital 16 of the GDPR, must be regarded as being designed solely to exclude from the scope of that regulation the processing of personal data carried out by state authorities in the course of an activity which is intended to safeguard national security or of an activity which can be classified in the same category. It particularly regards activities having the aim of safeguarding the essential functions of the state and the fundamental interests of society. …
>
> 39. The exceptional situations laid down in Article 2(2) GDPR are not applicable. Clearview is a private party and not a member state, government body or authorized authority. For that reason, the exceptional situations laid down in Article 2(2) opening words and subsections (a), (b) and (d) GDPR cannot apply."

25. In these passages, the regulator cited as authority Case C-439/19 *Latvijas Republikas Saeima* which in turn cited *Schrems II* discussed further below. The AP then went on to detail the breaches of the EU GDPR and the calculation of the penalty (€30.5m).

[11] Autoriteit Persoonsgegevens, 'Dutch DPA imposes a fine on Clearview because of illegal data collection for facial recognition', available online. **[AB/486]**

B.3 Further jurisdictions

26. As far as Privacy International is aware, Clearview has not complied with any of the EU-based regulatory notices above. No doubt this is because Clearview maintains that it is not subject to the jurisdiction of these regulators, but Privacy International is not aware of any legal appeals in that regard.

27. In addition to the above notices, data protection authorities in Hamburg (Germany)[12] and Sweden[13] have taken certain more limited steps concerning Clearview. Moving beyond the EU, regulatory interventions and investigations have been commenced in Australia and Canada against Clearview,[14] seemingly without any insurmountable jurisdictional hurdles.

C LEGAL FRAMEWORK

28. The relevant legal provisions and case law are set out below. The key point from Privacy International's perspective is that the proper interpretive approach to the scope of the UK GDPR, following the UK's withdrawal from the EU, must be in conformity with the approach taken under the EU GDPR.

C.1 Material and territorial scope of the UK GDPR

(i) The EU GDPR

29. The EU GDPR deals with material scope (i.e. the subject matter or activities caught by the GDPR) in Article 2 as follows:

> "**Article 2**
>
> **Material scope**
>
> 1. This Regulation applies to the processing of personal data wholly or partly by automated means ...
>
> 2. This Regulation does not apply to the processing of personal data:
>
> (a) in the course of an activity which falls outside the scope of Union law;
>
> (b) by the Member States when carrying out activities which fall within the scope of Chapter 2 of Title V of the TEU[15];
>
> (c) by a natural person in the course of a purely personal or household activity;

[12] In January 2021, the Hamburg data protection authority issued an enforcement notice against Clearview ordering it to delete information about a particular German citizen. The regulator explained how Article 3(2)(b) of the EU GDPR was satisfied as part of its reasoning (§1) **[FTTB/1258]**.

[13] In February 2021, the Swedish data protection authority issued a penalty against the Swedish police authorities for using Clearview. **[FTTB/1261]**

[14] Office of the Privacy Commissioner of Canada, PIPEDA Report of Findings #2021-001 (2 February 2021).

[15] This is a reference to the EU's common foreign and security policy.

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

30. The exemptions above in Article 2(2) include matters such as household processing in Article 2(2)(c). Most relevantly, and as explained in more detail below, Article 2(2)(a) is an exemption concerned with topics outside the *competence* of the EU, namely national security within the EU Member States. Thus Recital 16 states that the Regulation does not apply to "*activities which fall outside the scope of Union law, such as activities concerning national security*" or "*the processing of personal data by the Member States when carrying out activities in relation to the common foreign and security policy of the Union.*"

31. The EU GDPR then provides for territorial scope in Article 3(1) and extra-territorial scope in Article 3(2) as follows:

"**Article 3**

Territorial scope

1. This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.
2. This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:
   (a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or
   (b) the monitoring of their behaviour as far as their behaviour takes place within the Union. …"

32. It is immediately obvious from this that the EU GDPR has express extra-territorial effect (cf. Response §§48(3)(i) and 107). It is concerned with data processing even if undertaken by foreign entities so long as one of the conditions in Article 3(2) is met. So, where the behaviour of EU citizens is monitored, then that is caught by Article 3(2)(b) and it is irrelevant where the processor or controller is domiciled.

33. Recital 24 states that processing by controllers or processors outside the EU "*should also be subject to this Regulation when it is related to the monitoring of the behaviour of such data subjects in so far as their behaviour takes place within the Union*" and that this requires ascertaining "*whether natural persons are tracked on the internet including potential subsequent use of personal data processing techniques which consist of profiling a natural person, particularly in order to take decisions concerning her or him or for analysing or predicting her or his personal preferences, behaviours and attitudes*".

34. The EU GDPR had applied directly in the UK when it was introduced in May 2018. At that time, the UK also introduced in parallel the Data Protection Act 2018 ("**DPA**") which, among other things, addresses matters outside the scope of the EU GDPR, such as processing for law enforcement or national security purposes in the UK.

(ii) The UK GDPR after Brexit

35. After the UK withdrew from the EU, the EU GDPR was "saved" in its entirety as retained EU law (now assimilated law) under s. 3 of the European Union (Withdrawal) Act 2018.

36. In order to cure deficiencies in the saved EU GDPR and the DPA, on exit day, a series of minor amendments were made pursuant to the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 ("**2019 Regulations**"). For instance, the retained GDPR was renamed as the UK GDPR under Regulation 2. Schedule 1 of the 2019 Regulations set out a series of amendments to the UK GDPR and Schedule 2 set out a series of amendments to the DPA.

37. The Explanatory Memorandum to the 2019 Regulations provided that the changes were intended to continue the operation of the EU GDPR on a new footing in the UK (§§2.1, 2.9; Response §27). In terms of scope, Articles 2 and 3 of the UK GDPR were amended so that Article 2(1) brings into scope processing which was previously out of the scope of EU law to ensure that the UK can continue to exercise competence in these areas in its own jurisdiction. But it continues to leave out of scope matters such as household data processing under Article 2(2):

> "**Article 2**
>
> **Material scope**
>
> 1. This Regulation applies to the automated or structured processing of personal data, including—
>
> (a) processing in the course of an activity which, immediately before IP completion day, fell outside the scope of EU law, and
>
> (b) processing in the course of an activity which, immediately before IP completion day, fell within the scope of Chapter 2 of Title 5 of the Treaty on European Union (common foreign and security policy activities).
>
> 1A. This Regulation also applies to the manual unstructured processing of personal data held by an FOI public authority.
>
> 2. This Regulation does not apply to—
>
> (a) the processing of personal data by an individual in the course of a purely personal or household activity;
>
> (b) the processing of personal data by a competent authority for any of the law enforcement purposes (see Part 3 of the 2018 Act);

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

38. Article 3 then sets out the territorial scope of the UK GDPR which adopts the logic of the EU GDPR:

"**Article 3**

Territorial scope

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

2. This Regulation applies to the relevant processing of personal data of data subjects who are in the United Kingdom by a controller or processor not established in the United Kingdom, where the processing activities are related to:

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

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

2A. In paragraph 2, "relevant processing of personal data" means processing to which this Regulation applies, other than processing described in Article 2(1)(a) or (b) or (1A)."

39. The Explanatory Memorandum to the 2019 Regulations indicated that, as regards territorial scope, no substantive changes were intended:

"2.14 This instrument maintains the data protection standards that currently exist under the GDPR and the DPA 2018 and introduces a newly merged regime for general processing activities (covering matters that were in and out of scope of the GDPR prior to Exit Day). It also maintains the extra-territorial scope of the GDPR, so that controllers or processors based outside the EEA which are processing UK residents' data for the purposes of providing goods and services or monitoring behaviour will continue to be covered by the UK GDPR, and extends this to cover such processing by controllers and processors in the EEA. A number of functions conferred on the European Commission by the GDPR will be transferred to the Secretary of State and/or the Information Commissioner. …

4.3 The GDPR as it applies to the UK, and the DPA 2018 insofar as it supplements the GDPR for the UK, apply to processing by controllers and processors who are established outside of the EEA in certain circumstances where they are processing data about individuals who are in the UK. After Exit Day, the UK GDPR and the DPA 2018 (as both amended by this instrument) will apply in the same way to processing by controllers and processors who are established outside of the UK. This will extend the extraterritorial application of the domestic framework to the remaining EEA Member States."

40. The amendments to Articles 2 and 3 operated so that, among other things, matters previously set out in the DPA and outside the scope of EU law (such as processing by public authorities) were brought within scope of the UK GDPR:

"A single general processing regime

> 7.6 The 'applied GDPR' is a separate regime created by in Chapter 3 of Part 2 of the DPA 2018. It extends GDPR-equivalent standards to personal data processing which is not covered by other parts of the DPA 2018 and is outside the scope of EU competence, and it includes appropriate exemptions for national security and defence purposes. When the UK leaves the EU, all data processing, such as this, will be outside the scope of EU law (though EU jurisprudence will continue to have effect in the circumstances set out in section 6 of the EUWA).
>
> 7.7 To simplify matters at the point of exit, this instrument creates a single regime for data processing currently regulated by the GDPR and the 'applied GDPR'. Regulation 5 of the instrument makes clear that merging the 'applied GDPR' regime with the GDPR regime does not itself affect interpretation of processing for purposes that were outside the scope of EU competence prior to Exit Day and excludes the application of EU jurisprudence to such processing post-Exit where it did not apply to it pre-Exit (consistent with section 6(3)(b) of the EUWA). The amendments to Article 2 (Material scope) of the GDPR made by paragraph 4(2) of Schedule 1 to this instrument make clear that the newly merged regime covers matters that were outside the scope of EU competence prior to the UK's departure from the EU. …
>
> Territorial scope
>
> 7.9 Article 3 of the GDPR extends the regulation to data controllers and processors who are based outside of the EEA, but are processing personal data of people within the EEA in connection with the offering of goods and services to them or for monitoring purposes. Paragraph 5 of Schedule 1 of the instrument [amending Article 3] retains this principle in the context of the UK. In practice this means that the UK GDPR will apply to a controller or processor who is based outside of the UK, but is processing personal data of people within the UK in connection with the offering of goods and services to them or for monitoring purposes. This entails extending the scope of the current regime (which currently apply extraterritorially to controllers and processors outside of the EEA) to certain processing by controllers and processors established within the EEA after the UK's Exit."

41. To summarise, Articles 2 and 3 of the UK GDPR should be read as a whole and consistently with the relevant provisions in the EU GDPR. The provisions are not identical but the reason for this is that in the UK it was necessary to: (i) clarify that the UK was able to regulate as to issues outside of EU competence under Article 2; but (ii) maintain the substance of the EU territorial scope provisions so far as they apply to foreign controllers or processors under Article 3. The way this was achieved was that Article 2(1)-(1A) covers all processing activities, even those previously outside the scope of EU law, and then Article 3 excludes "out of scope of EU law" activities insofar as they are conducted by controllers outside the UK.

C.2 Interpretation must be consistent with EU law

42. Despite the complex legislative route, in substance the same extra-territorial effects are produced. The First Tier Tribunal was therefore right to conclude that, though the legislative route has changed, the question remains the same (Judgment §97). This appears to be common ground (ICO Skel §71).

43. This is consistent with the fact that the UK GDPR generally reflects Parliament's intention to preserve the substance of the EU GDPR law within the domestic legislation rulebook[16] and its clear intention that assimilated EU case law applies to interpreting the provisions.[17] If further support is needed for the importance of continuity it may be found in the fact that the protection of core concepts from the EU GDPR in the UK GDPR is a foundation of the EU's "adequacy decision" that permits data flows from the EU to the UK.[18]

44. It follows that there are two stages to the analysis on this appeal:

(1) First, the key concept in Article 3(2)(b) is that – even if the controller or processor is based outside the UK – their processing activities are covered by the UK GDPR if they relate to "*monitoring of behaviour*" in the UK. This is a provision with express extra-territorial effect based on the substance of the data processing activities and their impacts on UK data subjects and follows the approach taken in the EU.

(2) Second, the key concept in Article 3(2A) is that the UK GDPR does not cover activities of foreign controllers where their activities were previously outside the scope of EU law. This was necessary so that, given the extra-territorial effects on the EU, there was no incursion into issues that the EU legislature would not have intervened in.

C.3 Relevant guidance and case law

(i) Article 2(2)(a) of the EU GDPR

45. In *Schrems II*, which concerned bulk surveillance by the US, the Grand Chamber explained that Art. 2(2)(a) should be read narrowly to cover only situations where EU Member States are engaged in national security activities:[19]

> "80. By its first question, the referring court wishes to know, in essence, whether Article 2(1) and Article 2(2)(a), (b) and (d) of the GDPR, read in conjunction with Article 4(2)

---

[16] "the UK Parliament decided that from IP Completion Day the content of the GDPR should remain part of English law, with certain modifications and amendments": *R (Delo) v ICO* [2023] EWCA Civ 1141 §11 (Warby LJ), citing his earlier judgment in *R (Open Rights Group) v Secretary of State for the Home Department* [2021] EWCA Civ 800 §§5, 12-13.

[17] Under s. 6(3) of the European Union (Withdrawal) Act 2018, as amended by the Retained EU Law (Revocation and Reform) Act 2023.

[18] Commission Implementing Decision (EU) 2021/1772 of 28 June 2021 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by the United Kingdom (dated 28 June 2021 and due to expire on 27 December 2025).

[19] Case C-311/18 *Data Protection Commissioner v Facebook Ireland and Maximillian Schrems* [2021] 1 WLR 751, 861-862.

> TEU, must be interpreted as meaning that that regulation applies to the transfer of personal data by an economic operator established in a Member State to another economic operator established in a third country, in circumstances where, at the time of that transfer or thereafter, that data is liable to be processed by the authorities of that third country for the purposes of public security, defence and State security.
>
> 81. In that regard, it should be made clear at the outset that the rule in Article 4(2) TEU, according to which, within the European Union, national security remains the sole responsibility of each Member State, concerns Member States of the European Union only. That rule is therefore irrelevant, in the present case, for the purposes of interpreting Article 2(1) and Article 2(2)(a), (b) and (d) of the GDPR. …
>
> 84. … As to whether such an operation may be regarded as being excluded from the scope of the GDPR under Article 2(2) thereof, it should be noted that that provision lays down exceptions to the scope of that regulation, as defined in Article 2(1) thereof, which must be interpreted strictly (see, by analogy, as regards Article 3(2) of Directive 95/46, judgment of 10 July 2018, *Jehovan todistajat*, C-25/17, EU:C:2018:551, paragraph 37 and the case-law cited).
>
> 85. … Such a transfer [from Facebook Ireland to Facebook Inc.] also does not fall within the exceptions laid down in Article 2(2)(a), (b) and (d) of that regulation, since the activities mentioned therein by way of example are, in any event, activities of the State or of State authorities and are unrelated to fields in which individuals are active (see, by analogy, as regards Article 3(2) of Directive 95/46, judgment of 10 July 2018, *Jehovan todistajat*, C-25/17, EU:C:2018:551, paragraph 38 and the case-law cited)."

46. Clearview has suggested that this case is of no relevance because it concerns an operator established in the EU.[20] But the Court's ruling as to the proper scope of Article 2(2)(a) – noting the invocation of the provision was in the context of third country national security activities at §80 above – is obviously plainly relevant.

47. By way of context, the "scope" of EU law is a concept with a specific and narrow meaning in the EU GDPR,[21] deriving from a long-standing principle that Member States have exclusive competence over national security in their own jurisdictions. In particular, Article 4(2) of the Treaty on European Union states that:

> "**Article 4**
>
> 1. In accordance with Article 5, competences not conferred upon the Union in the Treaties remain with the Member States.
>
> 2. The Union shall respect the equality of Member States before the Treaties … It shall respect their essential State functions, including ensuring the territorial integrity of the

[20] Clearview's Response to Privacy International's application to intervene at §13(1) **[UTB/278]**.

[21] Jay, *Data Protection Law and Practice* (5th ed) [4-007] ("A distinction has to be drawn between the power of the EU to legislate and the scope of the areas of activity caught by any legislation. In order for the EU to legislate it must have the power to do so. If it does legislate such legislation only applies to those areas of activity which fall within Union competence"); [20-002] ("A number of areas of Member State activity fall outside the scope of Union law entirely. Therefore, the processing of personal data for such activities is not covered by the GDPR. National security and defence fall into this category. Nor does the GDPR apply to the processing of personal data by competent authorities for law enforcement purposes; such processing is subject to Pt 3 of the DPA 2018 which is based on the LED").

> State, maintaining law and order and safeguarding national security. In particular, national security remains the sole responsibility of each Member State."

48. Even where national security is invoked, the exemption is not beyond the courts' scrutiny. As noted above, the exclusions are interpreted restrictively. Consistent with this, in a recent case, the Grand Chamber found that an Austrian Parliamentary Committee was not able to rely on the national security exemption given that its object was to investigate sources of political influence on a domestic police agency: Case C-33/22 *Österreichische Datenschutzbehörde v WK* [2024] 4 WLR 42 ("***DSB v WK***") §§37, 45-57. In particular, at §50, the Grand Chamber said as follows:

> "although it is for the Member States, in accordance with Article 4(2) TEU, to define their essential security interests and to take appropriate measures to ensure their internal and external security, the mere fact that a national measure has been taken for the purpose of protecting national security cannot render EU law inapplicable and exempt the Member States from the need to comply with EU law".

49. Thus the Court's approach shows that whether even an EU Member State's activity is truly a national security activity that is outside the scope of EU law requires careful scrutiny, and a case-by-case assessment of each processing activity.

(ii) Article 3(2)(b) of the EU GDPR

50. There is no directly relevant EU case law as to "*monitoring*" of behaviour, but helpful guidance may be gleaned from *Soriano v Forensic News LLC* [2022] QB 533 (and the relevant passages are correctly cited in ICO Skel §158 **[UTB/327]**).

51. Further guidance can be found in the European Data Protection Board Guidelines 3/2018 on the territorial scope of the GDPR ("**EDPB Guidelines**"), which describe Article 3(2)(b) as the "*targeting criterion*" (see pp. 13-16). The EDPB Guidelines have been explained by the Information Commissioner at ICO Skel §§7 and §184 **[UTB/286 and 334]**.

C.4 Relevance of other EU regulators' approaches

52. Given the applicable legal principles set out above, it is suggested that the approach in the EU – reflected in the five EU decisions noted above – is highly informative. The First Tier Tribunal gave short shrift to the decisions of other regulators on the basis that they were not binding (Judgment §79 **[UTB/53-54]**). But Privacy International does not argue that these decisions are binding by way of precedent. Rather, the decisions are highly relevant given that they address and rely on precisely the same provisions that apply in the UK. It follows that any material divergence in approach needs to be properly understood and

explained, whether on the basis that the other regulators' reasoning is not sound or because the text of the UK GDPR mandates a different result.

D SUBMISSIONS

D.1 Article 3(2A) and the "scope" of EU law

53. The Judgment interprets Art. 3(2A) UK GDPR in an overly broad manner, effectively exempting any entity engaged in any activity that might touch and concern national security. That is diametrically opposed to the proper approach which is to construe the derogation contained in that provision narrowly. It led the Tribunal to reach the puzzling result that Clearview's and its unnamed clients' processing, which imperil millions of data subjects' rights in the UK, are not subject to the safeguards that the legislature and courts have established over the years for precisely this type of processing.

(i) Article 3(2A) is a narrow exemption for EU Member States' national security

54. Understood properly in the broader context, Art. 2(2)(a) EU GDPR (equivalently, Art. 3(2A) UK GDPR) makes sense as a narrow exemption and not an immunity for all activities connected with foreign states or national security generally.

55. First, the UK GDPR expressly continues the use of an EU law concept ("*processing in the course of an activity which, immediately before IP completion day, fell outside the scope of EU law*"). It follows that the provision has to be interpreted by reference to that earlier regime and applicable case law.

56. As explained above, Article 3(2A) derives from Article 2(2)(a) which contains the principle in EU law that Member States have exclusive competence in respect of national security and so those topics fall outside the "scope" of EU law. This provision is concerned with the institutional competence of Member States vis-à-vis the EU deriving from the allocation of responsibilities in the Treaty on European Union.

57. It therefore follows that the activities of a third country are not protected by Article 2(2)(a) (equivalently Article 3(2A). The Grand Chamber in *Schrems II* expressly confirmed that US national security objectives could not be invoked under Article 2(2)(a) at §81 (extracted above). The Dutch regulator rightly followed this approach. It follows that, contrary to the Tribunal's judgment, countries as wide-ranging as Panama, Brazil, Mexico and the

Dominican Republic[22] are not entitled to avail themselves of this provision.

58. Second, and relatedly, there is simply no authority in EU law for conferring a blanket exclusion on a private actor when Article 2(2)(a) is narrowly focused on core state competencies and responsibilities (see Article 4(2) of the TEU read with *Schrems II* §§80, 85). It would be wrong to suppose that the UK GDPR takes a fundamentally different approach to private actors in this regard. Insofar as Clearview implicitly relies on an asserted *indivisibility* with its state clients to avoid the result (Response §§65, 67, 75, 79 **[UTB/116, 119, 120]**) then that is addressed below with regard to state immunity.

59. Third, even if Article 3(2A) applies, the exclusion must be interpreted restrictively (*Schrems II* at §84) and its invocation needs to be scrutinised carefully (*DSB v WK* at §50). The First Tier Tribunal assumed that all of Clearview's clients are engaged in national security activities. It failed to consider with sufficient precision and clarity, for example, whether they were in fact local law enforcement or immigration agencies whose activities may have little to do with national security properly so-called. That was an error.

60. The difference between law enforcement and national security activities is an important one. Law enforcement activities are exempt from the UK GDPR under Article 2(2)(c) but they are subject to a specific set of rules under the EU Law Enforcement Directive (implemented in the UK in Part 3 of the Data Protection Act 2018).[23] Clearview does not appear to accept that it is within the scope of the Law Enforcement Directive in respect of its law enforcement activities; rather, it seeks to invoke the national security activities of some of its clients as a general immunity to escape the effect of both regimes.

61. Finally, even if certain national security activities of a Member State fall outside the scope of EU law, those state activities are usually subject to scrutiny at a domestic level or under the ECHR. So even if UK intelligence services' activities are outside the scope of the UK GDPR, there is nonetheless provision for the protection of privacy rights in domestic legislation (e.g. Part 4 of the DPA or the Investigatory Powers Act 2016). In addition, when UK intelligence services are engaged in surveillance activities, their actions require a lawful basis and must satisfy the principles of necessity and proportionality under Article

[22] Judgment §24.

[23] The safeguards of necessity and proportionality are embedded into these provisions. The detailed rules have been considered in detail in cases such as *R (Bridges) v South Wales Police* [2020] EWCA Civ 1058 (facial recognition) and *Elgizouli v Secretary of State for the Home Department* [2020] UKSC 10 (transfer of information in connection with a terrorist investigation).

8 of the ECHR (e.g. *Big Brother Watch* [2021] ECHR 439 §§350-364). There is no equivalent regulation of private entities engaged in surveillance activities under domestic law or under the ECHR. This leaves a striking gap in protection for data subject rights.

62. As a result of this erroneous approach to Article 3(2A), the Judgment stands apart in uncritically allowing Clearview to rely on national security as a form of complete immunity irrespective of the actual data processing they are involved in. Indeed, the judgment means that Clearview are provided an absolute exemption, regardless of who engages their services. As a result, UK data subjects are left without any recourse under the UK GDPR (or any other avenue in domestic law or even under the ECHR).

(ii) No justification for divergence with EU

63. As set out above, the UK GDPR is designed to achieve the same result in the UK as would be achieved in the EU. But as a result of the Judgment, people in the UK are in a materially worse position than those in the EU, even though the relevant GDPR provisions are the same. There is no good reason for this divergence and it is unjustified given the clear legislative intention in favour of continuity.

64. The divergence is not merely a matter of legal inconsistency. It has real practical consequences for UK data subjects. They will be unable to invoke individual data protection rights against Clearview under the UK GDPR (including the right of access, the right of erasure, the right to object, the right to rectification and so on). For instance, the right of access, which employees of Privacy International exercised in relation to their data held by Clearview, enabled them to see what images of them Clearview had scraped, processed through its facial recognition algorithm and stored in its database. For one of them, it also revealed that Clearview had misidentified them as the copy of their data included a photo of a stranger, enabling them to exercise their right to rectification.

65. It is difficult to justify the outcome wherein UK data subjects are left without control over their own images and information which are being retained and analysed by Clearview on a grand scale. Not only is the Information Commissioner unable to take any enforcement action against Clearview, but individual rights to privacy, transparency and fair processing, apparently guaranteed by the UK GDPR, are rendered ineffective and non-justiciable.

(iii) No application of state immunity

66. The state immunity issue arises due to an error on the part of the First Tier Tribunal below conflating (i) principles of state immunity with (ii) the scope of EU law under Article 3(2A). The Information Commissioner had accepted that the UK GDPR would not apply to acts of foreign governments, but the First Tier Tribunal appeared to conflate this point with the ambit of Article 3(2A) (Judgment §14 **[UTB/38]**). The misstep can be seen clearly in Judgment §153 **[UTB/72]** where the Tribunal finds that acts of foreign states are outside the scope of EU law and therefore outside the scope of the UK GDPR.

67. Insofar as state immunities arise on this appeal, Privacy International respectfully makes the following points of principle:

    (1) The doctrine of state immunity has its roots in promoting comity and good relations between sovereign states. The underlying rationale is that equals do not have jurisdiction over each other.[24]

    (2) State immunity will prevent a foreign state from becoming a party to domestic proceedings without its consent. The doctrine confers immunity from suit over: (a) the head of state, (b) the government, or (c) a government department.[25]

    (3) The immunity extends to "separate entities" when they are acting in the "exercise of sovereign authority".[26] As far as companies are concerned, this usually covers state-owned corporations which exercise public powers on behalf of the state.[27]

    (4) There is a related, but distinct, "act of state" doctrine which prohibits a UK court from adjudicating on acts of a foreign state. But that doctrine has no application where the foreign state takes steps which cause harm in the UK.[28]

---

[24] "*Par in parem non habet imperium*", recently reaffirmed in *The Royal Embassy of Saudi Arabia (Cultural Bureau) v Costantine* [2025] UKSC 9 §37.

[25] This is encapsulated in ss. 1 and 14 of the State Immunity Act 1978.

[26] Section 14(2) of the State Immunity Act 1978.

[27] *Dicey, Morris & Collins* [9-015] ("There is no express requirement that such a separate entity be owned or controlled by the foreign State, but it would be a considerable extension of the doctrine of immunity to apply the notion of separate entity to *any* agent of the foreign State, and it is therefore suggested that a separate entity not owned or controlled by the State is not capable of acting in the exercise of sovereign authority for the purposes of s.14").

[28] *Shehabi v Kingdom of Bahrain* [2024] EWCA Civ 1158 §§68-70. Note also s. 5 of the State Immunity Act 1978.

68. These principles would, in many but not all situations, apply to prevent (e.g.) the US, or a federal agency, from becoming subject to this Tribunal's jurisdiction. But whether state immunity principles can apply to render Clearview immune to the jurisdiction of the Tribunal is an entirely different question that requires careful scrutiny.

69. On appeal, Clearview appears to embrace the state immunity reasoning to the extent that the *interpretation* of the UK GDPR should be informed by state immunity principles and comity considerations (see Response §§48(3)(i), 49 90). This is a surprising submission given that state immunity appeared to play no role in, and prove no obstacle to, the interpretation of five or more EU regulators who have issued notices against Clearview.

70. Privacy International endorses the submissions of the Information Commissioner on these issues (see ICO Skel §§84-108). In particular, the proper analysis must be that Clearview cannot avail itself of state immunity without having to prove closely how it is an "emanation" of a particular state. Indeed, all the evidence points the other way:

    (1) First, Clearview is a privately owned, profit-making commercial enterprise which can be sued in its own right without requiring any foreign state to submit to the jurisdiction of the UK courts. Indeed, the state immunity doctrine recognises that states can *consent* to jurisdiction but there is simply no avenue for such consent in this case because Clearview is purporting to assert state immunity itself.

    (2) Second, Clearview provides services to different types of organisations, which may or may not be "states" or "government departments" in the relevant sense.[29] The First Tier Tribunal failed adequately to analyse: (i) the nature of each of Clearview's clients, (ii) their connection to national security activities; and (iii) the powers and authorities granted to Clearview by its clients. A detailed analysis is required at the minimum to understand whether Clearview is acting "*under colour of state authority*" in its activities.[30] State immunity would require considering the differences between (e.g.) a local police department, a border protection force, or a national security agency, but no such nuance is disclosed by the Judgment.[31]

---

[29] For example, the Terms of Service do not contain any clear restriction on the identity or the function of the user so as to limit it to state activities in the furtherance of national security **[FTTB/575ff]**.

[30] *Jones v Ministry of Interior (Kingdom of Saudi Arabia)* [2007] 1 AC 270 §74.

[31] Clearview has previously advertised its services to a range of clients plainly not limited to states engaged in national security activities. This was addressed in the PI Complaint at §5. In addition, Clearview itself advertises its functionality for a range of purposes, see, e.g., the case study concerning Nashville International Airport

(3) Third, even if Clearview exclusively provides services to foreign states, that would not necessarily bring it within the scope of state immunity. In this case, Clearview apparently provides services to more than one foreign state, which makes it highly improbable that it would be exercising sovereign authority in respect of national security on behalf of all of them. The far more likely inference is that it is an independent contractor without any sovereign powers at all.

71. This issue is particularly important to Privacy International given its years of work investigating the use of surveillance technologies by governments, law enforcement agencies, and private actors around the world. The surveillance practices of American state authorities in particular, which represent the majority of Clearview's clients, have been the subject of considerable concern from privacy advocates and European courts and resulted in many iterations of specialised safeguards.[32]

72. The increasing use of private corporations to assist foreign states with their national security and policing activities brings this issue into sharp focus and a careful resolution of the issues is required. For instance, in a personal injury claim brought against the Kingdom of Saudi Arabia ("**KSA**") in the UK, which involved the installation of Pegasus software on the claimant's phone, the High Court held that KSA (i.e. the state itself) could not rely on state immunity. In the course of his reasoning, ~~Robin~~ Julian Knowles J said he was prepared to accept that the act of installing the Pegasus software was an official act (*jure imperii*) rather than a private act (*jure gestionis*).[33] But that did not mean state immunity applied to those acts. This decision – while concerned with a rather different claim – shows that even states need to demonstrate how they can rely on state immunity under the relevant rules rather than simply assert it on the basis of national security.

73. Finally, it may be instructive to note in this regard that in the US, the Ninth Circuit Court of Appeal found against an Israeli private surveillance corporation which purported to rely

[FTTB/517] and Clearview's website which refers to categories as broad as "Law Enforcement, Government, Banking, Transportation, Payments, Visitor Management, Security and Authentication" **[FTTB/1146]**.

[32] See *Schrems v Data Protection Commissioner and another* [2016] Q.B. 527 ("*Schrems I*" which concerned the Safe Harbour) and *Schrems II* (discussed above) which concerned the Privacy Shield. The most recent statement of the EU with respect to US surveillance methods is the Commission Implementing Decision EU 2023/1795 of 10 July 2023 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate level of protection of personal data under the EU-US Data Privacy Framework (the "EU-US Data Privacy Framework").

[33] *Al-Masarir v Kingdom of Saudi Arabia* [2022] EWHC 2199 (QB) §77.

on state immunity in *Whatsapp v NSO*. While the relevant state immunity laws in the US are slightly different, Privacy International endorses the following analysis:[34]

> "NSO is a private corporation that designs spyware technology used by governments for law enforcement purposes. According to NSO, its Pegasus technology is a program that was "marketed only to and used only by sovereign governments" …
>
> NSO is a private corporation that provides products and services to sovereigns—several of them. NSO claims that it should enjoy the immunity extended to sovereigns because it provides technology used for law-enforcement purposes and law enforcement is an inherently sovereign function. Whatever NSO's government customers do with its technology and services does not render NSO an "agency or instrumentality of a foreign state," as Congress has defined that term. Thus, NSO is not entitled to the protection of foreign sovereign immunity. And that is the end of our task."

74. Put shortly, from Privacy International's perspective, it is vital that the doctrine of state immunity is not used in an unprincipled way to circumvent the clear extra-territoriality provisions in the UK GDPR and the concomitant rights of UK data subjects.

D.2 Article 3(2)(b) and "monitoring behaviour"

75. This issue arises under the "Additional Reasons" advanced by Clearview to cross-appeal the Judgment. Privacy International does not make any submissions on the procedural history of this point (ICO Skel at §§16-17 **[UTB/288]**). The submissions below make additional points in support of the Information Commissioner on the substance of Article 3(2)(b).

(i) The Judgment

76. On this issue, Privacy International respectfully endorses the careful reasoning of the First Tier Tribunal to the effect that Clearview's activities relate to monitoring behaviour in the UK (Judgment §§40, 59, 111-112, 142-144 **[UTB/44, 49, 62, 70]**).

77. In particular, as the Tribunal observed, Clearview's technology is related to monitoring behaviour because it enables identifying: (i) where a person is; (ii) what they are doing; (iii) what they have said; (iv) who they relate to or associate with; (v) and how this changes over time (i.e. tracking developments over time). This shows that both stages of processing (both gathering and scraping the data and then the searches run on it) are "*related to the monitoring of behaviour*" of UK data subjects (Judgment §§118-121 **[UTB/64-65]**).

---

[34] Opinion of Judge Forrest dated 8 November 2021 in *WhatsApp Inc. v NSO Group Technologies Limited*, (Case 4:19-cv-07123). An application to the US Supreme Court was dismissed in January 2023. WhatsApp ultimately succeeded on the merits in December 2024.

(ii) Clearview's activities relate to the monitoring of behaviour

78. In order to avoid duplication on this topic, Privacy International agrees with the submissions of the Information Commissioner as to the proper interpretation of Article 3(2)(b) in ICO Skel §§156-218 **[UTB/326-345]** and adds the following points in support.

(1) First, Clearview's position on appeal involves fundamental inconsistencies. On the one hand, it accepts the finding at Judgment §136 that it is a joint controller with its clients for the second stage of processing. It also argues that it is *so closely aligned* with its state clients that it can rely on state immunity. And yet, at this stage of the analysis under Article 3(2)(b), it contends that it has no part in monitoring behaviour of data subjects.

(2) Second, the functionality of the technology enables widespread and invasive surveillance, and this should inform the purposive interpretation of Article 3(2)(b):

(a) The Information Commissioner has set out the wide-ranging data and metadata that Clearview collects and deploys for the benefits of its clients (see the Information Commissioner's skeleton argument at §§31-41 **[UTB/293-298]** and Judgment §§47, 56 **[UTB/46, 48)**. Given the commercial object of Clearview's technology, it then becomes artificial to find that Clearview's activities do not even "relate to" the monitoring of behaviour.

(b) More generally, the contemporary practice of social media surveillance or open source surveillance (known as "**OSINT**" and "**SOCMINT**") is not benign in nature. In European human rights law, it is well-established that the collection of even public information in a systematic way engages the right to privacy.[35]

[35] *Rotaru v Romania* (Grand Chamber) §§42-44. In that case, Romania "denied that Article 8 was applicable, arguing that the information in the RIS's letter of 19 December 1990 related not to the applicant's private life but to his public life. By deciding to engage in political activities and have pamphlets published, the applicant had implicitly waived his right to the "anonymity" inherent in private life. As to his questioning by the police and his criminal record, they were public information." But the Court concluded that "public information can fall within the scope of private life where it is systematically collected and stored in files held by the authorities. That is all the truer where such information concerns a person's distant past. In the instant case the Court notes that the RIS's letter of 19 December 1990 contained various pieces of information about the applicant's life, in particular his studies, his political activities and his criminal record, some of which had been gathered more than fifty years earlier. In the Court's opinion, such information, when systematically collected and stored in a file held by agents of the State, falls within the scope of "private life" for the purposes of Article 8 §1 of the Convention. That is all the more so in the instant case as some of the information has been declared false and is likely to injure the applicant's reputation."

Privacy International has made submissions about this in other proceedings.[36]

(3) Third, Privacy International again relies on the reasoning of the EU regulators described above. At least five regulators have independently analysed Article 3(2)(b) against Clearview's technology and found that it applies in their respective jurisdictions. As explained above, to reach the opposite result in the UK would be surprising and, it is suggested, unjustifiable.

79. It is respectfully submitted that these broader factors are relevant because they show that *processing of this kind* is likely to be the kind of processing that the EU GDPR and UK GDPR were intended to capture.

(iii) Clearview is not operating a search engine that aggregates public information

80. Clearview contends that its activities do not relate to the monitoring of behaviour. One of its key arguments is that it simply *aggregates* publicly available information. It does not "*monitor*" people in the sense of engaging in live surveillance. It is akin to a search engine (Response §§31-32, 120 **[UTB/103, 131]**).

81. With respect, Privacy International has long been sceptical of these arguments: see PI Complaint §§63-68. Such a characterisation is wholly contrary to Privacy International's experience as a privacy rights campaigner and technical specialist. As explained in the PI Complaint, this technology goes far beyond ordinary users' experience of social media or search engines like Google. This is because:

(1) A person does not reasonably expect that images or information about them from public websites and social media will be systematically harvested, their biometric markers identified, and then the information joined up together with other clues about them online to build a facial recognition profile with a range of their photos and details. Usually, sharing on social media is within the control of the relevant individual. Clearview's subsequent use of this data for its own commercial purposes is likely to come as a surprise: such processing is of a totally different nature.

[36] For example, in March 2021, Privacy International intervened in the ECtHR in the case of *Salman Butt v UK* (Application no. 32946/20) which concerned the Home Office's use of social media information. It was argued there that the repurposing of social media data by authorities "for purposes that go 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 relates to personal data revealing political opinions" (§23 of the written intervention, available online).

(2) A photo of a person walking down the street or from CCTV could be used to search and then identify and de-anonymise them. It is important to note that unlike Google which requires a name for a search, using Clearview the searcher needs only a photo of a person to work out who they are and then learn other information about them. That not only impairs privacy online but in the physical world. It also inhibits free speech and participation on the internet once it is known that (no matter what you choose to call yourself online) someone could join the dots in this way.

(3) Clearview runs a sophisticated system which the individual in question cannot run a search on to work out if they are part of it. Nor can they exercise any rights of removal or correction (again unlike Google or other social media websites). All of the processing is "behind the scenes" as far as the individual is concerned.

82. Drawing these threads together, it is respectfully submitted that Clearview's attempts to downplay the invasive and far-reaching effects of its technology are entirely implausible. The wording of the provision ("*monitoring the behaviour*") is plainly broad enough to cover the technology operated by Clearview and sold to its clients for a profit.

E CONCLUSION

83. First, the Additional Reasons of Clearview should be rejected. The First Tier Tribunal was plainly correct to conclude that Clearview's activities related to monitoring behaviour under Article 3(2)(b) and therefore came within the extra-territorial reach of the UK GDPR. Second, the appeal of the Information Commissioner should be allowed. Otherwise, the Judgment will create an unjustifiable lacuna in the enforcement of the UK GDPR and prevent people in the UK from exercising any rights in respect of the harvesting and searching of their own images and personal data.

MARIE DEMETRIOU KC
AARUSHI SAHORE
Brick Court Chambers

AWO

27 May 2025