

IN THE COURT OF APPEAL (CIVIL DIVISION)
ON APPEAL FROM THE UPPER TRIBUNAL
(ADMINISTRATIVE APPEALS CHAMBER)
[2025] UKUT 319 (AAC)

Appeal no. CA-2026-000226

B E T W E E N:

CLEARVIEW AI INC

Appellant

-and-

THE INFORMATION COMMISSIONER

Respondent

-and-

PRIVACY INTERNATIONAL

Intervener

SKELETON ARGUMENT
for hearing on 19 - 21 October 2026

*References to the First-Tier Tribunal's Judgment are in the form **FTT** §*

*References to the Upper Tribunal's Judgment are in the form **UT** §*

*References to the Appellant's skeleton are in the form **CV** §*

*References to the Respondent's skeleton are in the form **ICO** §*

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 this right against incursions from surveillance technology.
2. In this appeal, Privacy International intervenes in support of the Respondent (the “**Commissioner**”) to argue that the material and territorial scope of the UK General Data Protection Regulation (“**UK GDPR**”) apply to the data processing activities of the Respondent (“**Clearview**”).
3. Consistently with its approach in the Upper Tribunal below, Privacy International focuses its intervention on Ground 3, which raises the question of whether Clearview’s data processing activities are outside the scope of the UK GDPR by dint of the fact that they

form part of services provided to foreign state clients. This ground of appeal raises legal issues as to: (i) the proper interpretation of Article 2(2)(a) of the EU GDPR (and equivalently Article 3(2A) of the UK GDPR); and (ii) international law principles such as state immunity and comity.

4. It is important to emphasise at the outset that Clearview has abandoned the “intersectional” argument that it ran below, namely that its own processing falls outside the material scope of the EU and UK GDPR by virtue of its “intersection” with the processing carried out by its foreign state clients (see UT §§197-214). However, Clearview seeks in this appeal to resurrect a version of this argument. It now submits that the monitoring carried out by its foreign state clients falls outside the scope of Article 2(2)(a) and should accordingly be regarded as a nullity. Accordingly, Clearview says, its own processing falls outside the scope of the legislation as there is no monitoring to which it can attach.
5. Clearview’s submission is misconceived. For the reasons developed in more detail below, Privacy International contends that:
 - (1) Clearview’s new argument fails as a matter of straightforward statutory construction. Both Article 2 and Article 3(2)(b) are concerned with the circumstances in which processing falls within the material and territorial scope of the UK GDPR. They are not concerned with determining the applicability of the UK GDPR to monitoring. It does not matter where or by whom the monitoring takes place in order for processing to fall within the scope of the UK GDPR.
 - (2) In any event, the Upper Tribunal correctly concluded that Article 2(2)(a) has a narrow meaning relating to the division of responsibilities between the EU and its members. This is well-established in EU case law. The provision does not apply to the provision by Clearview of services to third countries. See UT §§190-196.
 - (3) The Upper Tribunal was also correct to conclude that processing by third countries falls outside the UK GDPR not as a result of Article 2(2)(a) but as a result of the application of independent principles of public international law. The Upper Tribunal correctly concluded that Clearview was unable to avail itself of those principles. See UT §§215-219.

- (4) The effect of Clearview’s new interpretation of the UK GDPR is to circumvent the proper application of those public international law principles. The reason this matters, from Privacy International’s perspective, is that the public international law principles draw clear boundaries between private entities and the state, whereas Clearview’s approach seeks to blur those boundaries.
6. The remainder of this skeleton argument proceeds as follows. The relevant background from Privacy International’s perspective is set out in **Section B**. The legal framework is summarised in **Section C**. Privacy International’s submissions on Ground 3 are set out in **Section D**.

B RELEVANT BACKGROUND

7. Privacy International’s general expertise and experience are set out in its application to intervene and are not repeated here.¹ But there are two points of background from Privacy International’s perspective of which the Court should be aware.
8. First, over five years ago, Privacy International submitted a complaint to the Commissioner asking it to take action against Clearview for breaches of the UK GDPR.² This followed Privacy International’s own investigations whereby data subject access requests by Privacy International staff revealed that their images and names were held by Clearview (§21). The complaint provided a detailed explanation of Privacy International’s understanding of Clearview’s technology (§§6-7) and set out why it contravened various provisions of the UK GDPR (§§36-110).
9. The complaint included the following points as to the applicability of the UK GDPR:
- (1) In terms of territorial scope, the complaint argued that Clearview’s activities were caught by Article 3(2)(b). It was argued that Clearview “*engaged in monitoring of the behaviour of data subjects within the UK*” (§§15, 22). That point is covered by Ground 1 of the appeal, as to which Privacy International endorses the Commissioner’s submissions.

¹ The Court of Appeal’s Order acknowledges Privacy International’s expertise at para. 1.

² Privacy International, ‘Submission to the Information Commissioner – Request for assessment of processing operations by Clearview AI, Inc.’ (27 May 2021), available [online](#).

- (2) As to material scope, Privacy International did not know of, and did not expect there to be, any basis for Clearview relying on Article 2(2)(a) to avoid the application of the UK GDPR. Privacy International therefore simply noted that there was no reason for the Commissioner to “*reach a different conclusion*” from other EU regulators because the applicability of the UK GDPR “*follows the same principles as the EU GDPR*” (§26). That overarching submission is maintained on this appeal under Ground 3.
10. Second, five different EU data protection authorities have sought to take enforcement steps against Clearview under the EU GDPR: (i) CNIL in France, (ii) AP in the Netherlands, (iii) DSB in Austria, (iv) GDPB in Italy; and (v) HDPa in Greece. Privacy International was the originator of the complaint giving rise to the French decision and drafted the others before they were translated and filed by local organisations. These authorities, like the Commissioner, relied on Article 3(2)(b) of the EU GDPR to bring Clearview within territorial scope, and have not found Clearview to be exempt due to the nature of its clients.³ As far as Privacy International is aware, Clearview has not complied with any EU enforcement actions or penalties, nor has it appealed these decisions.
11. The Upper Tribunal declined to consider three EU regulators’ decisions on the basis that it would not permit the introduction of new factual evidence that had not been before the First-Tier Tribunal (see UT §§42-44) but Privacy International does not seek to rely on these decisions as evidence of facts. They are relevant as legal background. This is because Clearview accepts that the EU and UK GDPR are identical on the questions before the Court: CV §11. If that is right, then one would expect the approach to be consistent across the EU and UK, whereas Clearview’s interpretation leads to a divergence.
12. It is difficult to see how Clearview could properly maintain its objection to the admissibility of these decisions before this Court in circumstances where it seeks to rely

³ See (1) Commission Nationale de l’informatique et des Libertés, ‘*Restricted Committee Deliberation No. SAN-2022-019 of 17 October 2022 concerning CLEARVIEW AI*’; (2) Autoriteit Persoonsgegevens, ‘*Dutch DPA imposes a fine on Clearview because of illegal data collection for facial recognition*’ dated 16 May 2024; (3) Österreichische Datenschutzbehörde, ‘*Bescheid Spruch*’ dated 9 May 2023; (4) Garante per la Protezione dei Dati Personali ‘*Ordinanza ingiunzione nei confronti di Clearview AI - 10 febbraio 2022 [9751362]*’; (5) Hellenic Data Protection Authority, ‘*Decision 35/2022 – Imposition of fine on Clearview AI, Inc*’ dated 13 July 2022. Only the Dutch regulator expressly considered Article 2(2)(a) and found that it did not apply to exempt Clearview from the EU GDPR.

on new evidence of the foreign language versions of the EU GDPR (CV §§62-63). It would obviously be inappropriate for Clearview to invite the Court to place weight on that evidence whilst simultaneously arguing that the Court is precluded from having regard to decisions of regulators and courts which actually apply those foreign language versions of the same legislation. Moreover, Clearview mounts an argument based on its evidence of the Spanish language version of the EU GDPR whilst neglecting to mention that a Spanish court found that Article 3(2)(b) did apply to Clearview, a matter Privacy International has only become aware of in preparation for this appeal.⁴

13. Privacy International's position is straightforward: this Court is (obviously) not bound by the approach of any EU data protection authority or court, but it ought to be on notice of the potential divergence between the UK and EU when engaging with the issues before it. It should also be cautious about relying on cherry-picked foreign law advice without reference to the relevant European decisions and judgment.

C LEGAL FRAMEWORK

C.1 The EU GDPR

Material Scope

14. The EU GDPR deals with material scope 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 TEU⁵;

⁴ Judgment of the Audiencia Nacional of 27 June 2024 (Chamber for Contentious-Administrative Proceedings, First Section) Appeal No. 0002185/2021. The Spanish data protection authority, AEPD, declined to take any steps against Clearview on the basis that Article 3(2)(b) was not applicable to Clearview but this was overturned by the Court on appeal, in part by relying on the reasoning of the French regulator.

⁵ Chapter 2 of Title V of the TEU covers the EU's Common Foreign and Security Policy.

- (c) by a natural person in the course of a purely personal or household activity;
 - (d) by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences
- 15. Article 2(1) is broad and unqualified. It brings into scope, in principle, data processing overseas or processing conducted by public authorities.⁶ Then, as a counterweight to the breadth of Article 2(1), a list of exceptions is set out in Article 2(2)(a) to (d).
- 16. The exceptions in Article 2(2) of the EU GDPR can be traced back to Article 3(2) in the predecessor legislation, the Data Protection Directive 1995 (“**DPD**”):⁷

Article 3

Scope

1. This Directive shall apply to the processing of personal data wholly or partly by automatic means ...
2. This Directive shall not apply to the processing of personal data:
 - in the course of an activity which falls outside the scope of Community law, such as those provided for by Titles V and VI of the Treaty on European Union⁸ and in any case to processing operations concerning public security, defence, State security (including the economic well-being of the State when the processing operation relates to State security matters) and the activities of the State in areas of criminal law,
 - by a natural person in the course of a purely personal or household activity.

Part of the first indent of Article 3(2) of the DPD has been transposed into: (i) Article 2(2)(a) of the EU GDPR which concerns “*scope of Union law*”; and (ii) Article 2(2)(b) of the EU GDPR which concerns the EU’s common foreign and security policy.⁹ The second indent is the household exemption now found in Article 2(2)(c) of the EU GDPR.

17. At the heart of Ground 3 is Article 2(2)(a) which concerns matters outside the “*scope of Union law*”. This phrase is a term of art in EU law regarding the division of responsibilities

⁶ Case C-33/22 *Österreichische Datenschutzbehörde v WK* [2024] 4 WLR 42 §§32, 36, 38.

⁷ Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

⁸ As the Upper Tribunal explained at UT §59, at the time, Title V was concerned with the responsibilities of the Union and the Member States in respect of Common Foreign and Security Policy and Title VI addressed Police and Judicial Cooperation in Criminal Matters.

⁹ Case C-439/19 *B v Latvijas Republikas* [2022] 1 CMLR 9 §64.

between the EU and its Member States as set out in the Treaties.¹⁰ While the ordinary language of Article 2(2)(a) might suggest that it is a generic carveout for all matters over which the EU legislature has no competence, the case law shows that this phrase has a much more specific and narrow meaning.¹¹

18. Most recently, the Grand Chamber in *Österreichische Datenschutzbehörde v WK* summarised the parameters of Article 2(2)(a) as follows:¹²

37. It is apparent from the court’s case law that the exception provided for in article 2(2) of the GDPR must be interpreted strictly (*B v Latvijas Republikas*, para 62 and the case law cited). In that context, the court has previously had occasion to state that article 2(2)(a) of that Regulation, read in the light of recital (16) thereof, is 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 ...

46. The activities having the aim of safeguarding national security for the purposes of article 2(2)(a) of the GDPR encompass, in particular, those that are intended to protect essential state functions and the fundamental interests of society (*B v Latvijas Republikas* [2022] 1 CMLR 9, para 67 and *Komisija za zashtita* EU:C:2022:813, para 40).

47. In accordance with article 4(2) TEU, such activities remain the sole responsibility of the member states (see *BK v Slovenija* (Case C-742/19) EU:C:2021:597; [2022] 1 CMLR 19, para 36).

19. As explained in the passage above, the paradigm activity of Member States falling outside the scope of Union law are their national security functions. This is reflected in Recital 16 of the EU GDPR (“[t]his Regulation does not apply to ... activities which fall outside the scope of Union law, such as activities concerning national security”) and derives from

¹⁰ The “scope of EU law” is a concept that arises in other areas of EU law as well. For example, general principles of EU law and the Charter of Fundamental Rights apply to Member States only when they are acting in the scope of EU law (see e.g. Case C-617/10 *Aklagaren v Fransson* [2013] 2 CMLR 46 §§19-23).

¹¹ Case C-101/01 *Lindqvist* [2004] QB 1014 §§43-44; Case C-439/19 *B v Latvijas Republikas* [2022] 1 CMLR 9 §§64-68; Case C-311/18 *Schrems II* [2021] 1 WLR 751 §§80-85.

¹² Case C-33/22 *Österreichische Datenschutzbehörde v WK* [2024] 4 WLR 42. The *WK* case post-dates Brexit and is therefore not binding on the Court but it is highly persuasive given the context that the “scope of Union law” is a reference to an EU law concept that has been deliberately maintained by Parliament retaining reference to it in the UK GDPR. See further s. 6(1)-(2) of the European Union Withdrawal Act 2018 (as amended).

Article 4(2) of the Treaty on European Union (“*in particular, national security remains the sole responsibility of each Member State*”).

20. For the avoidance of doubt, the reference to “national security” in this context is limited to Member States’ national security activities, not those activities whenever they are conducted by any person or any country. That is because, as noted above, the scope of Union law is a concept relevant to the allocation of responsibilities as between the EU and its members. Accordingly, in *Schrems II*, the Grand Chambers clarified that Article 2(2)(a) had no relevance to the national security activities of a third country:¹³

81. ... 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. ...

21. If further support were needed for the above proposition, it can be found in Article 16(2) of the Treaty on the Functioning of the European Union, which is the legal basis for the EU GDPR and the EU Law Enforcement Directive (“*The European Parliament and the Council ... shall lay down the rules relating to the protection of individuals with regard to the processing of personal data ... **by the Member States** when carrying out activities which fall within the scope of Union law*”). Indeed the EU Law Enforcement Directive uses the same language as the EU GDPR (Article 2(3)(a) excludes from scope data processing “*in the course of an activity which falls outside the scope of Union law*”) and the CJEU has taken a consistent approach to find that it is primarily a reference to the national security activities of Member States.¹⁴
22. Article 2(2)(a) is thus a narrow exception principally concerned with individual Member States’ national security activities, in recognition of the fact that the EU has no competence over those matters vis-à-vis the Member States. The provision is quite obviously not concerned with extra-territoriality; nor is it an attempt to codify any particular

¹³ Case C-311/18 *Schrems II* [2021] 1 WLR 751 §81.

¹⁴ Case C-118/22 *Direktor na Glavna direktsia ‘Natsionalna politsia’ pri MVR – Sofia* [2024] 3 CMLR 25 [38].

international law principles concerning state immunity or comity. Those principles, as explained below, arise independently of the EU GDPR.

Territorial Scope

23. After material scope is established under Article 2, one then proceeds to territorial scope in Article 3, which provides 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. ...
24. Article 3(2) provides expressly for a degree of extra-territorial effect where EU data subjects' rights are at stake.¹⁵ This is a carefully calibrated regime for extraterritoriality: each of the limbs bring foreign controllers' processing into scope only where there is a sufficient nexus with EU data subjects, whether by reference to offering goods or services into the EU (Article 3(2)(a)) or monitoring behaviour of data subjects in the EU (Article 3(2)(b)). Further guidance can be found in the European Data Protection Board Guidelines 3/2018 ("**EDPB Guidelines**") as set out in UT §119.

C.2 The UK GDPR after Brexit

25. On exit day, the EU GDPR was "saved" under s. 3 of the European Union (Withdrawal) Act 2018, renamed the UK GDPR, and immediately amended pursuant to the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 ("**2019 Regulations**"). These were minor amendments intended to

¹⁵ This was a new provision with no forebear in the DPD which was introduced to ensure comprehensive protection of EU data subjects' rights. See *Soriano v Forensic News LLC* [2022] QB 533 §79 and the European Data Protection Board Guidelines 3/2018 on the territorial scope of the GDPR ("**EDPB Guidelines**") p. 4.

continue the effective operation of the EU GDPR in the UK after exit day (Explanatory Memorandum §§2.1, 2.9, 6.1).

26. Article 2 of the UK GDPR now provides:

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). ...
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; ...

27. Article 3 of the UK GDPR now provides:

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).

28. To summarise, Article 2(1)(a) brings into scope matters outside the scope of EU law (to enable the UK to regulate those issues within the UK) but then excludes them under Article 3(2)-(2A) where foreign controllers are concerned. The Explanatory Memorandum provides that the intention was to maintain the extra-territorial scope of the UK GDPR

(§§2.14, 7.7 and 7.9).¹⁶ Accordingly, while these amendments are complex, the end result is intended to be the same as the EU GDPR. That has been uncontroversial throughout these proceedings (see e.g. FTT §97, UT §57, ICO §13, CV §11).

C.3 State immunity, comity and extra-territoriality

29. International law principles and related doctrines arise only indirectly on this appeal, but it is important to understand their proper application when considering Clearview’s submissions on Ground 3. In particular:

(1) **State immunity.** State immunity is a principle of international law which has its roots in promoting comity; the rationale is that equals do not have jurisdiction over each other.¹⁷ Further:

(a) It is a personal immunity which prevents a foreign state from becoming a party to domestic proceedings without its consent.¹⁸

(b) The doctrine confers immunity from suit over: (a) the head of state, (b) the government, or (c) a government department.¹⁹

(c) The personal immunity extends to “*separate entities*” including companies when they are acting in the “*exercise of sovereign authority*”.²⁰ This is similar to an agent acting under the colour of public authority.²¹

¹⁶ This is also consistent with the fact that the UK GDPR reflects Parliament’s intention to preserve the substance of the EU GDPR law within the domestic rulebook: “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 “*Par in parem non habet imperium*”, recently reaffirmed in *The Royal Embassy of Saudi Arabia (Cultural Bureau) v Costantine* [2025] UKSC 9 §37.

¹⁸ *Belhaj v Straw* [2017] AC 964 §§14 (Lord Mance); 182 (Lord Sumption).

¹⁹ This is encapsulated in ss. 1 and 14 of the State Immunity Act 1978.

²⁰ Section 14(2) of the State Immunity Act 1978; *Dicey, Morris & Collins* [9-015].

²¹ *Jones v Ministry of Interior of Saudi Arabia* [2007] 1 AC §74 (Lord Hoffmann).

- (d) The reason that these third parties are able to benefit from the immunity is so that it is not possible to circumvent the state's immunity by suing its servants or agents.²²
- (2) **Act of state.** There is a related “act of state” doctrine which prohibits a UK court from adjudicating on acts of a foreign state acting within its proper jurisdiction. This strictly arises under common law rather than as a matter of international law.²³
- (3) **Extra-territoriality.** Deriving in part from the overarching principle of comity, there is a presumption in domestic law that legislation is not intended to have extraterritorial effects, subject to contrary indication.²⁴ It is of limited relevance in the present case given that Article 3(2) expressly determines the extraterritorial effect of the EU and UK GDPRs.
- (4) **EU law.** As far as EU law is concerned, its institutions are also obliged to observe principles of international law such as state immunity. That is made express in Article 3(5) of the TEU which provides that the EU will contribute to the “*strict observance*” of international law.²⁵ It follows that the EU legislature and courts will respect the sovereignty of third country states but this does not mean that its legislation will always be territorial, e.g. extraterritorial effects are recognised in the regulation of competition law.²⁶

D PRIVACY INTERNATIONAL'S SUBMISSIONS ON GROUND 3

D.1 Clearview's articulation of Ground 3

30. Clearview contends at CV §§10(2), 70-74 that:

²² *Jones v Ministry of Interior of Saudi Arabia* [2007] 1 AC §10 (Lord Bingham).

²³ *Shehabi v Kingdom of Bahrain* [2026] UKSC 25 §§106-107.

²⁴ *R (KBR Inc) v SFO* [2022] AC 519 §§24-25.

²⁵ Case C-266/16 *Western Sahara Campaign* §47 (“the European Union is bound, in accordance with settled case-law, when exercising its powers, to observe international law in its entirety, including not only the rules and principles of general and customary international law”).

²⁶ Joined Cases 89/85 and others *Ahlström Osakeyhtiö and Others v Commission* [1988] ECR 5193, §§14-18, rejecting an argument that the prohibition on anti-competitive conduct was contrary to public international law principles since it applied to foreign companies where their conduct had an effect on the market in the EU.

- (1) The behavioural monitoring activities of its foreign state clients are, by their nature, outside the scope of EU law and therefore outside the scope of the UK GDPR;
 - (2) It necessarily follows from (1) that any processing activities of Clearview relating to those behavioural monitoring activities are similarly outside the scope of the UK GDPR. That is because there is simply no behavioural monitoring to which the legislation can attach.
31. This argument has evolved considerably. As far as Privacy International can discern:
- (1) Ground 3 is framed as an argument about the interpretation of Article 3(2)(b). Clearview submits that, because its processing relates to monitoring by foreign states, it thereby falls outside the territorial scope of the UK GDPR. So while Clearview does not seek to suggest that it has a claim to state immunity, it relies on the nature of its foreign state clients and their activities to argue that the EU and UK GDPRs must be read down so as not to undermine the sovereign functions of those states.
 - (2) Ground 3 is premised on the success of Ground 1. If this Court rejects Ground 1 and finds that Clearview is engaged in behavioural monitoring, then the appeal must be dismissed. That is because Clearview (rightly) does not seek to argue that it should benefit from the cloak of state immunity or any similar exemption for its own activities. See how the point was clarified at UT §§216-219.
 - (3) Ground 3 is premised on the failure of Ground 2. In other words, the arguments under Ground 3 assume that Clearview’s processing activities “*relate to*” behavioural monitoring where that monitoring is being undertaken by Clearview’s clients (Clearview calls this the “Client-Centred Finding”). Clearview uses this framing as the foundation for the submission that there is simply no behavioural monitoring to which the UK GDPR can attach.
32. Privacy International supports the submissions of the Commissioner on Grounds 1 and 2. To the extent that Ground 3 arises for consideration, it should be rejected, because there is no basis for Clearview’s suggested interpretive constraint in any ordinary rules of construction under domestic or EU law. Moreover, it is an attempt to circumvent the strictures of the international law principles which do apply.

D.2 Proper construction of Article 3(2)(b)

33. Clearview’s argument fails as a matter of straightforward construction of Article 3(2)(b). That provision brings within the territorial scope of the EU GDPR processing of personal data of persons in the EU by a processor or controller established outside the EU where the processing activities relate to the monitoring of the behaviour of data subjects within the EU. The UK GDPR provides for analogous extraterritorial effect.
34. The issues that arise under Article 3(2)(b) are accordingly:
- (1) Is the data processor or controller established outside the EU?
 - (2) If so, is it processing personal data of persons in the EU?
 - (3) If so, do those processing activities relate to the monitoring of their behaviour taking place in the EU?

If the answer to these questions is ‘yes,’ then the processing falls within the territorial scope of the EU and UK GDPRs by virtue of Article 3(2)(b).

35. There is nothing in Article 3(2)(b) that lays down any requirements as to the nature or location of the monitoring or the person conducting the monitoring. That is a complete answer to Clearview’s argument on construction. But the difficulties with Clearview’s arguments go further. The implication of Clearview’s argument is that the Article 3(2)(b) should be interpreted and applied differently depending on the identity of Clearview’s client. If Clearview was providing services to another company who was engaged in behavioural monitoring, then Article 3(2)(b) would apply. But if a state conducts behavioural monitoring then the Court must read down the provision by introducing the fiction that it never occurred. This is so even where it has been established that Clearview and its clients are joint controllers when searching Clearview’s database (see FTT §§135-137). This is an entirely unworkable approach including because it is rife with uncertainty as to how it would apply in future cases. The more straightforward reading, which does not require introducing fictions for different types of clients, must be the correct one.
36. It should be noted that a somewhat analogous argument was rejected by the Supreme Court in *US v Nolan*. In that case, the US had made an interpretive argument in favour of a “tailored exemption” in employment legislation to give effect to state immunity (without

actually relying on state immunity).²⁷ The Supreme Court rejected the submission as follows:

27. ... The submission would amount, in effect, ... to reading domestic legislation as subject to an exception or as inapplicable, at least *prima facie*, in relation to a foreign state in any circumstances where the foreign state could rely on a plea of state immunity, to avoid the adjudicative processes of another state in which proceedings had been brought against it. I do not accept that there is any such principle. It would make quite largely otiose the procedures and time for a plea of state immunity. ...

38. ... carried to its logical conclusion it would mean that all legislation should, however clear in scope, be read as inapplicable to a foreign state in any case where the state could plead state immunity. That would elide two distinct principles, and, as noted already, very largely make redundant a plea of state immunity at least in respect of any statutory claim.

37. The position should be *a fortiori* where a private entity is invoking the fact that its clients are states to create a tailored exemption for itself in the UK GDPR.

D.3 Article 2(2)(a) or public international law principles

38. In any event, even if it were necessary (or meaningful) to determine whether the monitoring by Clearview's clients fell outside the scope of the UK GDPR, it is important to determine on what basis that is so.
39. Clearview professes indifference as to the basis on which its clients fall outside the scope of the UK GDPR (CV §§10(2), 74) but, for the reasons explained below, the correct analysis is that Clearview must rely on the public international law principles which apply independently of the UK GDPR. It is important not to conflate the two.
40. First, for the reasons set out in §§17-22 above, Clearview's reliance on Article 2(2)(a) is misplaced. The phrase "*scope of Union law*" as it is used in the EU GDPR is a term of art concerned with the division of responsibilities between the EU and its members. The primary focus of Article 2(2)(a) is the national security functions of the Member States and it is not concerned with Clearview's third country client state such as the US. The Upper Tribunal was right to conclude that Article 2(2)(a) has a well-established meaning within EU law which does not assist Clearview (UT §§186, 191).

²⁷ *United States of America v Nolan* [2016] AC 463 §27.

41. Second, Clearview argues that the activities of third countries such as the US are self-evidently outside the scope of EU law (CV §74). But these arguments, relying on the ordinary meaning of “scope of EU law”, prove too much. As a general matter, persons or activities in (e.g.) Brazil are not within the scope of EU law. But that cannot be the meaning of “scope of EU law” because it is clear from the text of the EU GDPR that some persons and activities in Brazil *do* come within scope through Article 3(2). See EDPB Guidelines Examples 19 and 20. However, given the sweeping nature of Clearview’s submission as to the scope of EU law, it has no way of explaining why foreign corporations are within the scope of EU law but foreign states are outside the scope of EU law. The only reason to distinguish between these two is because of their nature, with foreign states having a sovereign function, but this comes back to the application of public international law principles, not the meaning of the scope of EU law. To put the point another way, if Clearview was only providing its services to private corporations in the US, it would not be able to argue that those activities were excluded by Article 2(2)(a) even though as a matter of ordinary language they would be outside the scope of EU law.
42. Third, foreign states such as the US cannot be the subject of enforcement under the EU GDPR, but that has nothing to do with the text of Article 2(2)(a). Such entities are immune to enforcement or court proceedings of the UK or EU due to state immunity. Similarly, the act of state doctrine would prevent this Court sitting in judgment of the sovereign acts of the US within its territory. But it is not necessary for these immunities to be “read into” the scope provisions in the UK GDPR to reach this result – they are overriding and independent principles.
43. This is an important point because once the Court clears away Clearview’s submissions about “*scope of Union law*”, then it is necessary to consider precisely how Clearview could “piggyback” off the identity of its clients to evade the application of the UK GDPR. The correct approach would be for Clearview to demonstrate that its nexus with the foreign state(s) was so close that it was exercising sovereign authority. Or it would need to explain why this Court would be at risk of sitting in judgment of the sovereign acts of foreign states. Those questions would arise in domestic and EU law by reference to the international law principles. Instead, these concrete questions are bypassed through the assertion that anything to do with the activities of foreign states is *ipso facto* outside the scope of EU law.

44. Clearview oversimplifies these complex issues by arguing in the abstract that it is “artificial” for US police forces to be able to use in-house facial recognition technology but not be able to use Clearview’s services (CV §73). As to this, there is obviously no prohibition on US police forces using Clearview’s technologies; the effect of the Notices is simply that Clearview is required to comply with the UK GDPR when providing those services to the US police. But the key point is that the distinction between the US state and the commercial operators who provide services to it is an important and sound distinction. That distinction follows precisely the principles of international law wherein the activities of state agents are not immune from suit *unless* the agent is acting under the colour of public authority. States cannot expect all their contractors (e.g. caterers providing catering services to a state department) to be immune from foreign enforcement merely because they act for the state; something more is required.
45. Privacy International maintains its submissions that foreign state activities are only outside the reach of the UK GDPR because of general principles of international law. It follows from this that Clearview must properly articulate the basis on which it can seek to avoid the UK GDPR by reference to those public international law principles. So if a private company controller is *prima facie* brought within scope (if it satisfies territorial scope), that result can only be displaced through reliance on state immunity or the act of state doctrine. Under the properly applicable principles, a detailed examination would be required to establish that the controller is truly acting under state authority (*jure imperii*), such that enforcing the Notices would impinge on state sovereignty. This would require understanding the precise law enforcement or national security functions of the state when using the database. It would also invite examination of how Clearview could conceivably exercise public authority on behalf of multiple different states at once.²⁸ Applying the correct principles, it appears highly unlikely that a private firm in these circumstances could invoke state immunity or any equivalent principles.

²⁸ FTT §24 records that Clearview had provided services to a variety of states including Panama, Brazil, Mexico and the Dominican Republic. As far as Privacy International is aware, Clearview also provides services to the US, Ukraine, Brazil and Argentina at present.

D.4 Clearview’s new interpretive argument seeks to circumvent principles of public international law

46. In the tribunal below, Clearview had not attempted to meet the test of state immunity or any equivalent public international law principle but instead made its so-called “intersectional” construction argument which has now been replaced with its new interpretive argument.
47. Clearview’s new argument is wrong as a matter of straightforward statutory construction as explained above. But if Clearview seeks to fall back on principles of comity to advance its argument, this would be wholly inadequate. As the Upper Tribunal explained, the limited extraterritoriality in the UK GDPR does respect comity: UT §§174, 193, 216-219. Beyond that, there are specific doctrines which could in principle avail Clearview such as state immunity or sovereign act of state. But no foreign states are impleaded by the Notices or this appeal; nor are their activities actually affected. None of these principles can support the contorted interpretation of Articles 2 and 3 for which Clearview contends. On the contrary, Clearview’s interpretive argument seeks to circumvent these well-established principles.

E CONCLUSION

48. Privacy International is grateful for the opportunity to intervene in this appeal. For the reasons set out above, the appeal on Ground 3 should be dismissed.

MARIE DEMETRIOU KC
AARUSHI SAHORE
Brick Court Chambers

AWO

26 August 2026