EIP

Clearview AI victorious on a fact specific exemption but what does this judgment mean for the extra territorial effect of the UK GDPR

Clearview AI victorious on a fact specific exemption but what does this judgment mean for the extra territorial effect of the UK GDPR, in particular Article 3(2)(b)?

(Clearview AI Inc v The Information Commissioner [2023] UKFTT 00819 (GRC))

Summary

- On 17th October 2023 the First-tier Tribunal ("**Tribunal**") overturned the UK Information Commissioner's Office ("**ICO**") UK GDPR and GDPR Enforcement Notice ("**EN**"), and a Monetary Penalty Notice ("**MPN**") issued to Clearview AI Inc. ("**Clearview**"), a US-based facial recognition company.
- Despite the Tribunal finding that Clearview did carry out data processing relating to monitoring the behaviour of people in the UK, the Tribunal ruled that the ICO "did not have jurisdiction" to issue the EN or the MPN on Clearview because their relevant customers were all foreign law enforcement agencies. As such, it fell into a specific exemption for foreign law enforcement (contained in Article 3(2A) UK GDPR / Article 2(2)(a) GDPR).
- On 17 November 2023 the ICO issued a statement confirming that they are seeking permission to appeal the judgment of the Tribunal on the basis that the ICO consider that Clearview itself was processing the personal data of UK residents and not purely for foreign law enforcement purposes. As of the date of this article,

the ICO awaits the Tribunal's decision.

To read the full article, please scroll down.

What is Clearview AI?

Clearview is a private US-based company that at the date of the ICO decision provided a facial recognition platform exclusively for non-UK/EU criminal law enforcement and national security agencies. Clearview's online database has more than 20 billion images of people's faces and data from publicly available information on the internet and social media platforms all over the world (which the ICO claimed, and Clearview accepted, is likely to include a substantial amount of the personal data of UK residents given the high number of UK internet and social media users).

The Clearview service allows their customers to upload an image of a person to Clearview's app, (the "**Probe Image**") which is then checked for a match against all the images in the database. The app then provides a list of images that have similar characteristics with the photo provided by the customer, with a link to the websites which were the source of those images. However, those individuals "probed" are not informed that their images were being collected or used in this way.

Background

Clearview does not offer its services to UK organisations; nevertheless, on 18 May 2022, the ICO issued to Clearview an MPN in the amount of £7,552,800 million for processing personal data in breach of UK GDPR and an EN ordering them:

a. to stop obtaining and using personal data of UK residents that is publicly available on the internet, and
b. to delete the data of UK residents from its systems.

The ICO concluded that as Clearview has customers in other countries and the company is using personal data of UK residents to provide services to them, the UK GDPR applied on the basis of the application of Article 3(2)(b) which provides (emphasis added):-

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

p3

On 20 June 2022, Clearview challenged the ICO's decisions, disputing the ICO's characterisation of the service provided by Clearview and its jurisdiction to issue the notices.

Note that as the relevant period covered by the notices straddled the BREXIT transition period, the legal position was governed by the GDPR and the UK GDPR (post transition period). However, for the purposes of this article we shall focus on UK GDPR (the underlying rationale for the decision is the same for both GDPR and UK GDPR).

The Judgment

The Tribunal was asked to consider whether Clearview's service fell within the territorial scope of the UK GDPR (with GDPR "**the Regulations**"). The Tribunal set out the questions it had to address as follows:

1. As a matter of law, could Article (3)(2)(b) UK GDPR (see above for the wording) apply where the monitoring of behaviour is carried out by a third party (i.e. the foreign law enforcement agency) rather than the data controller?

The Tribunal concluded that it could apply.

2. As a matter of fact, did the processing of personal data by Clearview relate to monitoring by either Clearview itself or by its client's?

The Tribunal concluded that as a matter of fact the processing of data by Clearview was related to the monitoring of behaviour by Clearview's clients – Clearview was not itself monitoring the behaviour of the data subjects in question.

3. Does the processing by Clearview fall outside UK GDPR as a result of the meaning of Article 2(2)(a) UK GDPR and/or otherwise not "relevant processing" for the purposes of Article 3(2)(b) UK GDPR. If so UK GDPR would not apply to the processing in question? UK GDPR provides in relevant part (emphasis added):

- Article 3(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)**"
- Article 2(1)(a): "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."

The effect of Article 3(2A) when read with Article 2(1)(a) UK GDPR is that the processing described in Article 2(1)(a) is excluded from the scope of Article 3(2)(b). This mirrors the

position under GDPR (Article 2(2)(a)). Included within the types of processing thus excluded is the processing of personal data for law enforcement purposes.

p4

As a result, the Tribunal concluded that the processing by Clearview fell outside the scope of UK GDPR (and GDPR) as it is not "relevant processing" for the purposes of Article 3(2)(b) UK GDPR..

Consequently, the Tribunal concluded that the ICO did not have jurisdiction to issue the notices because:

a. the UK GDPR (like the GDPR) does not cover the data protection activities of foreign governments/national security ; and
b. Clearview currently only offers its services to foreign governments; as such its activities are to be treated for the purposes of UK GDPR (and GDPR) as being the activities of foreign governments.

Additional Considerations

In its judgment, the Tribunal also shed light on some other points that have wider application, especially for data matching services.

- **Scope of Article 3(2)(b) UK GDPR** – The extra territorial effect of Article 3(2)(b) applies if the relevant processing activities relate to monitoring of the behaviour of UK residents, but the Tribunal went on to explain that:
    - "**behaviour**" has a broader meaning than just a description of a person (e.g. name, date of birth, height, hair colour) it means information that "would reveal that the person is doing something" (paragraph 117). For example, a person's habits, such as what they drink.
    - "**monitoring**" includes tracking a person at a fixed point in time as well as on a continuous or repeated basis.
    - in this case, Clearview was not themselves monitoring UK residents because its processing was limited to creating and maintaining a database of facial images and biometric vectors. However, Clearview's clients were using its services for monitoring purposes. As such, Clearview's processing "**related to**" monitoring under Article 3(2)(b) and so would have been caught by UK GDPR but for the fact that the processing was carried out by foreign law enforcement agencies.

Meaning of "Joint Controller" – A company offering services like Clearview, could be considered a joint controller with its clients where both determine the purposes and means of processing. In this case, Clearview was a joint controller with its clients

because it imposed restrictions on how clients could use the services (i.e., limited to matters of law enforcement and national security) and determined the means of processing when matching the search image against Clearview's facial recognition database.

Commentary

Clearview's successful appeal from the ICO decision turns on the question whether all the processing it carries out is processing related to the monitoring of behaviour by foreign law enforcement agencies which is exempt from the application of UK GDPR and GDPR. In one sense this is a case specific question of fact which might in itself not be a significant development in the law (and may even be short-lived if the ICO is successful in its appeal). Without such a fact specific exemption, the processing of publicly available data of people in the UK for the purpose of monitoring their behaviour falls within the scope of the UK GDPR.

What is perhaps of greater interest in this judgment is what it could mean for the commercial use of large-scale identifying databases by non-UK companies that do not have Clearview's client base (i.e. foreign law enforcement). In this case, the Tribunal (and the ICO) made a broad assumption that Clearview's database contained UK data on the basis that it involved scraping the global internet and social media. As such, there is a risk now that any non-UK company that relies upon data from a company that could include data identifying UK residents could be subject to the UK GDPR merely by the nature of its use of the Internet and/or social media. Further, this judgment makes clear that a controller or processor may be caught by the extra-territorial scope of the UK GDPR on the basis that its processing activities relate to the monitoring of the behaviour of data subjects in the UK, even where that entity is not itself monitoring data subjects, but where its activities enable its customers to conduct such monitoring. This arguably represents a significant extension in the extra- territorial reach of UK GDPR and will increase the compliance burden on such companies as well as their clients.