What are the implications of Clearview AI's win?

Katie Hewson, Partner, Daniel Jones, Associate, and Nelson Kiu, with Stephenson Harwood LLP, analyse the UK Tribunal's recent Clearview decision and its implications for organisations and data protection professionals, including those outside of the UK who process the personal data of UK data subjects as part of their activities

In October 2023, Clearview AI Inc. ('Clearview') achieved a successful outcome at the First-tier Tribunal ('Tribunal') in its appeal against a fine of over £7.5 million imposed by the UK Information Commissioner's Office (the 'ICO') in May 2022.

Clearview, a US-based company, provides facial recognition software to law enforcement agencies and their contractors around the world. Its software allows customers to upload an image/images of individuals they want to identify (a 'probe image') and receive information about any matching images in Clearview's database, such as the website where the image was found, any text associated with the image and any metadata. Clearview's database contains billions of images scraped from the internet, including social media and news sites, without the consent of the individuals depicted.

In May 2022, the ICO issued Clearview with a Monetary Penalty Notice imposing a £7,552,800 fine, and an Enforcement Notice requiring it to delete and stop processing the personal data of any UK residents. The ICO found that by collecting individuals' images and associated information, storing them in its database and matching them to probe images, Clearview had processed UK residents' personal data without any lawful basis in breach of both the GDPR and UK GDPR.

Clearview appealed this decision to the Tribunal, arguing that the ICO did not have jurisdiction to issue the notices. The Tribunal agreed with Clearview and overturned the notices, but on a very narrow ground relating to the non-applicability of the GDPR and UK GDPR to foreign law enforcement activities. The Tribunal also concluded that if this ground had not applied, Clearview's activities would have been caught by the GDPR and UK GDPR, even though Clearview was not established in the EU or UK.

As the notices issued by the ICO covered the processing by Clearview over the period of the UK's transition away from the EU — where the GDPR, and thereafter the UK GDPR, were in application — the dispute concerned the proper interpretation of the material and territorial scope of both the GDPR and the UK GDPR.

The GDPR and UK GDPR apply to the processing of personal data by controllers and processors that are established in the EU or UK, as well as to those who are not established in the EU or UK but whose processing activities fall within the extraterritorial effect of the GDPR and UK GDPR (Article 3(2)). Controllers and processors outside of the EU or UK are within scope, to the extent that their processing occurs in the context of offering goods or services to, or monitoring, data subjects in the EU or UK (as applicable).

The basis for the appeal

Article 2 of the GDPR specifies that processing activities that fall outside of the scope of EU law, such as law enforcement and national security activities, are not covered by the GDPR. In the UK post Brexit, these excluded processing activities normally fall within the scope of Article 2 of the UK GDPR.

However, this is not the case when it comes to the application of the UK GDPR to non-UK entities under Article 3(2). Here, the UK GDPR only applies to 'relevant processing' by these entities, which is confined to processing within the scope of EU law as it stood immediately before IP completion day i.e. 31st December 2020, the day on which the UK exited the EU.

In effect, this excludes processing by non-UK entities, such as Clearview, from the scope of the UK GDPR where processing is carried out for law enforcement or national security purposes. This is on the basis that these processing activities would not be considered 'relevant processing' under Article 3 of the UK GDPR.

The Tribunal's application of Article 3(2) to Clearview's activities

In issuing the notices to Clearview, the ICO had held that the GDPR and UK GDPR applied to Clearview by virtue of part (b) of Article 3(2), which covers the processing of personal data of data subjects in the jurisdiction by a controller or processor not established in the jurisdiction, where the processing activities are related to the monitoring of their behaviour as far as their behaviour takes place within the jurisdiction. The Tribunal considered whether the various elements of Article 3(2)(b) of the GDPR and UK GDPR had been satisfied in relation to Clearview's activities.

(1) Monitoring of behaviour

The Tribunal began by considering whether the behaviour of UK data subjects in the UK had been monitored. It noted that the monitoring did not need to be carried out by Clearview itself, but could be carried out by a third party, such as Clearview's customers, as long as there was a link between Clearview's processing and the monitoring.

The Tribunal also explained that 'behaviour' relates to the doing of something by a person, rather than simply their characteristics, and that 'monitoring' could include establishing where a person is or was at a particular point of time; watching a person over time by repeatedly submitting probe images; or combining data from probe search results with information from other forms of surveillance. Monitoring did not have to be a repeated action; it could include a single incidence of monitoring behaviour.

Taking this into account, the Tribunal concluded that Clearview itself was not monitoring behaviour, as its process of creating and maintaining its database of images did not reveal anything about the behaviour of a person, but was an automated, mathematical exercise. However, Clearview's customers were monitoring behaviour, specifically that of the individuals who appeared in probe images, as they were seeking to identify facts about where those individuals were and who they associated with (among other things).

The Tribunal also held that it was more likely than not that this monitoring related to the behaviour of UK data subjects in the UK, as Clearview's customers could be investigating international activities.

(2) Processing personal data of UK data subjects

The Tribunal then considered whether Clearview was processing the personal data of UK data subjects. It accepted the ICO's argument that Clearview processed personal data through two types of activities: (i) creating and maintaining its database of images; and (ii) receiving probe images from clients, matching these images to images in its database and providing search results to clients.

It also accepted the ICO's argument that this processing was of personal data of UK data subjects, finding that: (i) Clearview's database contained personal data of UK data subjects, as the images and associated information could identify or relate to them; and (ii) vectors created from the images of UK residents and processed as part of the matching process were personal biometric data, as they were derived from the physical characteristics of a person and could be used to identify them.

(3) Data processing by Clearview 'related to' the monitoring of behaviour by its customers

Finally, the Tribunal considered whether Clearview's data processing was 'related to' the relevant monitoring of behaviour by its customers.

The Tribunal noted that there was no legislative definition of 'related to', but that it meant that there was a relationship between the processing of the individual's personal data and the monitoring of behaviour that was in issue.

The Tribunal found that such a relationship existed between Clearview's processing and the monitoring by its customers, as Clearview's customers could not carry out their monitoring without the processing carried out by Clearview in creating and maintaining the database. Further, the purpose of the processing involved in Clearview receiving probe images, matching these images to images in its database and providing search results was to enable Clearview's customers to carry out their monitoring.

The Tribunal's conclusion on the scope of the GDPR and UK GDPR

Although on the face of it, the requirements of Article 3(2)(b) of the GDPR and UK GDPR were therefore satisfied, the Tribunal ultimately concluded that Clearview's data processing did not fall within the scope of the GDPR or UK GDPR, as the GDPR and UK GDPR did not apply to data processing carried out as part of foreign law enforcement activities.

In relation to the GDPR, the Tribunal found that Article 2(2) operates to exclude from its scope certain types of data processing to which the law would otherwise apply, including the processing of personal data in the course of an activity which falls outside the scope of EU law, such as acts of foreign governments. As Clearview's processing was carried out for the purposes of criminal law enforcement and/or national security functions by non-EU law enforcement bodies and their contractors, it was outside the scope of the GDPR.

In relation to the UK GDPR, the Tribunal reached the same conclusion, but by a slightly different route, as the UK GDPR contains some additional provisions that reflect the UK's departure from the EU. The Tribunal found that Clearview's processing was not 'relevant processing' for the purposes of Article 3(2) of the UK GDPR, as it was processing that fell outside the scope of EU law immediately before IP completion day. As such, the Tribunal held that the UK

(Continued on page 8)

(Continued from page 7)

GDPR did not apply to Clearview's processing either.

The implications of the Tribunal's decision

The Tribunal's decision is significant for organisations and data protection professionals as it provides useful guidance on the interpretation and application of Article 3(2) of the GDPR and UK GDPR, which determines the extraterritorial effect of the EU and UK GDPR.

The decision also highlights the potential risks and challenges for entities not otherwise subject to the UK GDPR who process the personal data of UK data subjects as part of their activities, as the decision means that there is a risk they could be subject to the UK GDPR and the ICO's enforcement powers, depending on their activities. This is a particular risk for organisations which facilitate or enable monitoring of UK data subjects by others.

Clearview's data processing has been under focus elsewhere than the UK. In the EU, the Austrian Supervisory Authority held in May 2023 that Clearview must comply with the GDPR and was no longer allowed to collect and process images of data subjects in Austria for a biometric search engine. It also held that Clearview must delete all personal data processed for that purpose for lacking a valid legal basis, although no general ban of Clearview was issued. In July 2022, the Greek Supervisory Authority issued a similar decision against Clearview, ordering it to delete and stop processing data of data subjects in Greece and imposing a fine of €20 million.

Similar decisions against Clearview have also been made by the Supervisory Authorities in France and Italy in December 2021 and February 2022 respectively, which deemed it illegal for Clearview to process personal data of residents in those countries for lack of a valid legal basis under the GDPR. Compared to the UK, there seems to be a divergence in approach taken by the regulators. This was picked up on in a statement made by the non-profit privacy advocacy organisation NOYB, which stated that: "it is unfortunate that no general ban was issued. The case of the complainant is likely the same for everyone else in Austria. It seems that Clearview's processing is only considered illegal if you complain to the [Supervisory Authority]".

> ***"Organisations should therefore not assume that their processing activities automatically fall outside the scope of the GDPR or UK GDPR, but should carefully examine the relevant provisions and their applicability to their processing activities."***

Returning to the Tribunal's decision in the UK, there are several important implications.

First, the concept of 'monitoring of behaviour' is broad and flexible, and does not require a controller or processor to carry out the monitoring themselves, but could include enabling or facilitating the monitoring by a third party. The concept of 'behaviour' also covers more than just the characteristics of a person, but could include their location, associations, preferences or activities. The concept of 'monitoring' could include a single or repeated action, and could involve the use of different sources of data or surveillance. Organisations should therefore be aware of the potential scope of Article 3(2)(b) of the UK GDPR and assess whether their processing activities could amount to, or relate to, the monitoring of the behaviour of data subjects in the UK.

Second, the processing of the personal data of UK data subjects could include the collection, storage, analysis or disclosure of any information that could identify or relate to them, either directly or indirectly. This could include images, text, metadata or biometric data, such as facial vectors. Organisations should therefore ensure that they have a clear understanding of the types and sources of personal data that they process, and whether they could relate to UK data subjects.

Third, the relationship between the processing of personal data and the monitoring of behaviour does not need to be direct or causal, but could be indirect or incidental. The Tribunal adopted a purposive and contextual approach to determining whether the processing was 'related to' the monitoring, taking into account the nature and objectives of the processing and the monitoring. Organisations should therefore consider the purpose and context of their processing activities, and whether they could be linked to the monitoring of the behaviour of data subjects in the UK by themselves or by a third party.

Fourth, the exceptions and exclusions from the scope of the GDPR and UK GDPR are narrow and specific, and depend on the nature and context of the processing activities. The Tribunal found that Clearview's processing fell within an exception or exclusion from both the GDPR and UK GDPR, but only because it was carried out for the purposes of foreign law enforcement or national security activities, which are outside the scope of EU or UK law. Organisations should therefore not assume that their processing activities automatically fall outside the scope of the GDPR or UK GDPR, but should carefully examine the relevant provisions and their applicability to their processing activities.

Fifth, as the Tribunal's decision was based on the fact that Clearview's processing was not within the scope of EU law as at IP completion day, Clearview could seek to argue that it was not within the competence of EU Supervisory Authorities to enforce against it. This argument would be made on the basis that law enforcement-related processing is not within the scope of EU law. It remains to be seen the impact this will have on the

ongoing cases within the EU and EEA.

Final thoughts

The Tribunal's decision is certainly not the final word on the matter, as the ICO is seeking to appeal the decision. In a recent statement, the ICO said that that "the Commissioner considers the Tribunal incorrectly interpreted the law when finding Clearview's processing fell outside the reach of UK data protection law on the basis that it provided its services to foreign law enforcement agencies. The Commissioner's view is that Clearview itself was not processing for foreign law enforcement purposes and should not be shielded from the scope of UK law on that basis."

However, the decision is an important reminder of the complexity and importance of the extraterritorial effect of the GDPR and UK GDPR, and the need for organisations to comply with these laws when processing the personal data of data subjects in the UK.

Katie Hewson
Stephenson Harwood LLP
Katie.Hewson@shlegal.com