UK GDPR extraterritoriality: scope clarified as Clearview AI wins appeal

While the First-tier Tribunal has recently provided useful clarification of the wide scope of the extraterritoriality rules and other concepts in the retained EU law version of the General Data Protection Regulation (*679/2016/EU*) (UK GDPR), pursuing a regulatory enquiry or legal action against a foreign party with no establishment in the UK will be difficult, unless the party engages with UK proceedings like Clearview AI Inc (*Clearview AI Inc v Information Commissioner [2023] UKFTT 819 (GRC)*).

Fine overturned

Clearview is a US company that provides facial recognition technology to law enforcement agencies. The technology compares probe images that are uploaded by its clients against Clearview's database of images sourced from the internet, including social media platforms. The output includes images that are sufficiently similar to the probe image along with source URLs, associated text, links to social media profiles, and information known as camera EXIF data, such as shutter speed, model details, flash settings, colour, space, date and time.

On 23 May 2022, the Information Commissioner's Office (ICO) fined Clearview £7.5 million for breaching the UK GDPR, following similar actions against Clearview in Canada, Australia, Sweden and Italy (*see feature article "AI and automated decision making: to regulate or deregulate?", www.practicallaw.com/w-033-8467 and Briefing "Facial recognition technology: the risks unfold", www.practicallaw.com/w-033-4793*).

Clearview appealed and the tribunal held that the ICO did not have jurisdiction to issue enforcement notices because Clearview had no establishment, clients or servers in the UK and it provided services only to non-UK law enforcement authorities and not to any commercial organisations. This put its activities beyond the material scope of the relevant processing of personal data under Article 3(2A) of the UK GDPR.

Territorial scope

Entities that are not established in the UK may be caught by extraterritoriality provisions in Article 3(2) of the UK GDPR (Article 3(2)) if they offer goods or services in the UK or monitor the behaviour of individuals in the UK. The case against Clearview focused on the second limb.

The tribunal clarified that, in order to trigger the second limb of Article 3(2), the organisation does not need to actually monitor behaviour as long as its processing relates to the monitoring. This means that foreign processors that offer services to UK controllers may be subject to the UK GDPR even if they are not established in the UK or carrying on any behaviour monitoring, but nevertheless provide services that relate to behaviour monitoring.

While the substantive law of the UK GDPR will apply in these circumstances, this does not mean that the ICO will have an easy job procedurally pursuing foreign offenders, as its jurisdiction will likely be challenged by those parties and foreign courts.

Controller and processor

The tribunal found that Clearview is a data controller in relation to maintaining its database and a joint data controller with its clients in relation to returning search results to clients. This is because Clearview determines the purposes of processing by deciding which clients may use its services for the limited purpose of law enforcement. Both Clearview and its clients determine the means of processing as the clients upload the probe images and Clearview does the matching. The tribunal held that Clearview also acts as a processor in relation to both activities.

This means that Clearview would have to comply with the requirements of Part 3 of the Data Protection Act 2018 (DPA 2018) as a controller engaged in law enforcement processing if it were ever to offer its services to UK law enforcement authorities. However, it is debatable to what extent a commercial party like Clearview should be subject to those rules merely due to its clients' activities, and how it can benefit from and justify its activities under a regime that is intended for law enforcement authorities.

Monitoring online behaviour

The tribunal provides helpful guidance on the meaning of the terms "monitoring" and "tracking", which are used in recital 24 to the UK GDPR. Activities may result in monitoring and tracking even if they are not continuous (one-off monitoring will still count), not carried on with an intention to track, not carried out for the benefit of the controller or processor, and even if the data collected does not immediately exhibit the behaviour of an individual.

The tribunal considered that the word "behaviour" goes beyond mere identification or descriptive terms, such as the person's height, hair colour, age, name or date of birth. It stated that a description of a person's behaviour will include a verb. Behaviour also includes location, employment, playing a sport, who a person associates with and what they are wearing. It was the tribunal's view that the search results returned by Clearview's service revealed to clients aspects of the behaviour of individuals.

The tribunal stated that obtaining, or seeking to obtain, information of the nature provided by Clearview constitutes monitoring. However, decisions in this area are highly fact-specific; for example, using the alert feature to track the appearance of images on the internet over time could constitute monitoring. Therefore, some of Clearview's clients will be engaged in the monitoring of behaviour when using the service, while others will not be engaged in behaviour monitoring. Assuming the former scenario, the tribunal held that Clearview's activity will relate to the monitoring of behaviour under Article 3(2).

Automated indexing

The ICO claimed that the gathering of facial vectors created from personal data and indexing them according to their similarity is comparable to state surveillance and that Clearview is therefore monitoring behaviour. However, the tribunal held that this activity is an automated, mathematical exercise and is not within the scope of Article 3(2)(b).

While there is no doubt that this activity would constitute the processing of personal data, it does not result in the monitoring of behaviour (*Google Spain SL and Google Inc v Agencia Española de Protección de Datos and Mario Costeja González C-131/12; see News brief "Google decision: the right to be forgotten", www.practicallaw.com/3-568-9605*). The behaviour of a data subject is not used in the creation of the facial vectors or the indexing

of images according to those vectors. That processing by itself reveals nothing about the behaviour of a person.

However, referring to *Walter Tzvi Soriano v Forensic News LLC and others*, the tribunal noted that Clearview's processing is related to the monitoring carried out by its clients because the monitoring could not take place without the maintenance of Clearview's database and the purpose of Clearview's matching or search function was to enable the monitoring of behaviour carried out by Clearview's clients (*[2021] EWCA Civ 1952*). The tribunal concluded that Article 3(2)(b) can apply where the monitoring of behaviour is carried out by a third party rather than the data controller.

Takeaways from *Clearview AI*

The decision in *Clearview AI* might have been different if the ICO had pursued other arguments. The fact remains that Clearview did offer its services to commercial organisations up until its settlement with the American Civil Liberties Union on 4 May 2022 (*www.aclu.org/cases/aclu-v-clearview-ai*). Clearview also ran trials for UK-based law enforcement clients and, instead of relying on the UK GDPR, the ICO could have pursued an infringement of Part 3 of the DPA 2018. However, these points were neither pushed nor supported by evidence in this case.

The case shows the ICO's willingness to pursue alleged infringements in relation to high-risk processing, despite jurisdictional difficulties. The decision clarifies the far reach of the UK GDPR's extraterritoriality provisions. This is a warning to many foreign controllers and processors that might believe that the UK GDPR does not apply to them (*see box "EU extraterritorial enforcement"*).

The findings on the automated indexing of biometric data are interesting as they suggest some freedom for foreign organisations that build their services on the personal data of individuals in the UK. However, these activities could be considered as relating to the offering of goods or services in the UK and could trigger the other extraterritoriality limb under the UK GDPR.

It will be interesting to see if Clearview stands any chance of success in challenging similar fines received in other countries. Meanwhile, on 17 November 2023, the ICO announced that it is seeking permission to appeal the decision in *Clearview AI* (*https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2023/11/information-commissioner-seeks-permission-to-appeal-clearview-ai-inc-ruling/*).

EU extraterritorial enforcement

The subject of extraterritorial enforcement of the General Data Protection Regulation (*679/2016/EU*) has also been of interest to the European Data Protection Board. Its research report in 2021 concluded that not only do some EU member state supervisory authorities lack the power under local law to summon officials of foreign entities but, in the absence of any memorandum of co-operation or similar international law instrument, they would also likely fail in proceedings brought in foreign states against offending entities (*https://edpb.europa.eu/system/files/2023-04/call_9_final_report_04112021_en_0.pdf*).

Alexander Dittel is a partner, Maya de Silva is a solicitor, and Enea Aniaj is a trainee solicitor, in the Technology Practice at Wedlake Bell LLP.

