Listen world, Clearview will not degrade GDPR's extraterritorial reach, says English tribunal

English Upper Tribunal sided with the UK Information Commissioner (**ICO**) in its appeal[1] against a decision of the First-tier Tribunal which, operating under a material error in law, incorrectly concluded that Clearview's large scale profiling of the UK's entire population using biometric technology sat outside of the material and territorial scope of the General Data Protection Regulation (**GDPR**). This is indicative of how complex data protection cases involving novel technologies can become.

The decision confirms the expansive interpretation of the GDPR's extraterritorial provisions, putting to rest possible challenges under principles of comity and sovereign equality, e.g. laws of one country do not bind another. The ICO's power to take action against foreign operators is confirmed. Clearview is reported to be disappointed with the decision which interprets the GDPR so as to "*improperly seek to regulate how American companies serve the US government*".[2]

The decision reaffirms that, contrary to Clearview's submissions, the GDPR is indeed an "*all singing and all dancing*"[3] protection for data rights as is consistent with popular belief. The judgment discloses Clearview's extraordinary attacks on the GDPR's extraterritorial applicability, based on interpretation which the Upper Tribunal described as "*artificial*", not "*linguistically possible*" and at odds with a clear legislative intention and express wording of the GDPR.

Australian organisations must appreciate the higher risk of regulatory action when engaging in processes involving the handling of personal data of individuals in the UK or EU. Such processes will likely attract GDPR compliance requirements even if they are ancillary to another party's operations, e.g. an Australian service provider providing ancillary services to corporate clients in the EU, UK or elsewhere in the world.

Background

Clearview argued that the GDPR did not apply to it because, firstly, it is a foreign operator and its crawling of peoples' faces and contextual photos from the web to create detailed databases did not amount to monitoring of behaviour within Article 3(2)(b) of the GDPR's extraterritorial scope, and, secondly, once a law enforcement client used Clearview's service to make a person search, such processing was exempt from the material scope of the GDPR under Article 2(2)(a) on account of being

[1] The Information Commissioner - v - Clearview AI Incorporated - and- Privacy International NCN [2025] UKUT 319 (AAC) (link).
[2] Clearview AI sees red as UK tribunal sides with regulator over $10M GDPR fine, The Register (link).
[3] See Upper Tribunal judgment.

sovereign activity by a foreign state. The Upper Tribunal disagreed and confirmed the ICO had jurisdiction to issue to Clearview the enforcement and the monetary penalty notice in May 2022.

The decision clarifies that a strict interpretation applies to determining which activities of a foreign state might be exempt from the GDPR and whether private organisations might benefit from such exemption under principles of comity and sovereign equality; noting that these principles prevail over Article 2(2)(a) of the GDPR.

"Monitoring" of behaviour

Clearview argued its clients are those who engaged in behavioural monitoring and not Clearview. At that point, Clearview is not "*on the field*" and played no part in it. The GDPR's extraterritoriality provisions apply to the person "*responsible for the mischief*" of monitoring. It was argued that Clearview as an independent controller had no view of the client's onward use of its database and could not know if clients engaged in monitoring of behaviour. The Upper Tribunal disagreed and held that Article 3(2) applies to the processing of personal data of data subjects who are in the Union whether or not they are the same individuals as those to whom the goods or services are offered, providing the two activities are "*related to*" one another by way of a "*close connection*".

The term "monitoring" of behaviour is not defined in the GDPR. However, any interpretation predicated on "active" or "watchful" monitoring activity may be too narrow. The GDPR was intended to capture automated information gathering – such as Clearview's crawlers being extremely watchful and operating on "*a virtually constant basis*", far better than any human could.

Clearview's database of "*behaviourally rich*" images was held to be an "*ideal tool for behavioural monitoring*", going far beyond facial images. In an example search, the information included person's photos with the same child over time, photo with a possible female partner, location at some point in Memphis, USA, shown smoking and gesturing with his middle finger, shown drinking alcohol, shown performing musically at a specific time and place, shown performing a specific song, shown to have used social media, shown holding a large quantity of dollar bills, shown sitting in the driver's seat of a US car, shown with a handgun tucked into his belt or pocket, the subject of a police mugshot more than once. Gathering data in contemplation of the potential eventuality that someone will access it for monitoring may be enough to qualify as "monitoring" under the GDPR.

Foreign state activity is exempt

Article 2.2(a) exempts from the material scope of the GDPR "*an activity which … fell outside the scope of Union law*". This will apply to activities reserved by the state where no powers are conferred on the Union to act, respectful of comity principles.

The Upper Tribunal disagreed that Clearview's clients' processing was exempt under Article 2(2)(a) as this article "*deals only with the division of responsibility between the Union and its Member States, and is not about foreign states or private bodies providing services to foreign states at all*". However, Clearview's foreign state clients fell outside of GDPR due to comity principles. Private sector contractor clients could only be so exempt if they acted in exercise of sovereign authority and under state immunity, perhaps as an agent of a foreign state.

Clearview, not being an agent of the state, could not claim the exemption for its activities of building its database or offering the service to law enforcement clients for investigations. Clearview's counsel submitted that the GDPR must not be interpreted so as to compel foreign states to change the way they discharge their functions as such interpretation would amount to "legal heresy". The Upper Tribunal found these submissions "puzzling". A private operator cannot engage in activities that are quintessentially state functions, without a proper mandate.

Conclusion

This decision puts in serious doubt the lawfulness of law enforcement tools being developed by the private sector based on the covert collection of vast amounts of public data relating to individuals in the UK (and arguably, in the EU) which cannot be reconciled with the GDPR's data protection principles and the fundamental right to privacy (unless the developer acts as an agent of the state and complies with Part 3 of the Data Protection Act 2018).

The decision reaffirms the wide reach of the GDPR well beyond the UK's (and arguably, the EU's) territorial borders when it comes to the handling of personal data of people in the UK (or EU). Activities carried out abroad by a processor or controller which may be used by a third party to offer goods or services or monitor the behaviour of individuals in the UK (and EU) are subject to the GDPR, even if they do not relate to the same individuals. The GDPR's extraterritorial application is affirmed and there is no *de minimis rule* which allows foreign operators to escape the GDPR because of their activity's limited nature.

Alexander Dittel is a Principal in **Data Privacy, Cyber and Digital** at KHQ Lawyers