BCLP. Client Intelligent

Insights

PRIVACY SPEAKS: A CLEARER VIEW?

THE IMPACT OF RECENT LEGAL DEVELOPMENTS ON IMAGE SCRAPING, “MONITORING BEHAVIOUR” AND THE REACH OF THE UK GDPR

Jan 18, 2024

SUMMARY

Clearview AI Inc's successful challenge to the ICO’s £7.5 million fine focused on the limits of the UK GDPR’s jurisdictional reach, succeeding on the grounds that Clearview’s processing activities were outside the scope of the UK GDPR.

At the time of writing, we await confirmation of whether the ICO will be allowed to appeal. In the meantime, the decisions have provided some interesting clarifications around the application of data protection law to publicly accessible images. This comes at a time when the ICO is consulting on the application of UK data protection law to generative AI (including obtaining training data) and the UK government has dropped plans for a broad exception to current UK copyright rules, which would have permitted text and data mining of copyright protected works for AI training purposes.

THE ICO’S 2022 INVESTIGATION

In May 2022, the ICO fined Clearview AI Inc (a Delaware incorporated company) £7.5 million for its use of images of people in the UK to create a global online database of more than 3 billion images which could be used for facial recognition. The images were collected from the web and social media. By October 2022, the database reportedly contained over 20 billion images, with an estimated growth rate of 75 million images per day. Clearview does not have and did not have any establishment in the EU or UK and does not have any servers in the United Kingdom nor use any IP addresses in the UK.

The principal service offered by Clearview is through the use of facial recognition technology that makes a comparison of a “probe” image submitted by a client against images Clearview has copied from publicly available sources on the internet. The service is an internet-based search tool to which only Clearview clients have access. All of Clearview’s clients carry out criminal law enforcement and / or national security functions and use the service in furtherance of those functions. The Clearview terms of service state that users may only use the services for legitimate law enforcement and investigative purposes and are prohibited from using the services for a commercial purpose.

As well as a fine, the ICO issued an enforcement notice ordering Clearview to stop obtaining and using UK residents' personal data and to delete the data from its systems. The ICO found that Clearview:

- had not been fair and transparent in its use of UK residents' data (as they would not have been aware that their personal data was being used in this way);
- did not have a lawful reason for collecting the data;
- did not have a process in place to stop the data being retained indefinitely;
- failed to meet the higher standards required for biometric special category data; and
- had requested additional personal information, including photos, when asked by members of the public if they are on their database. This may have acted as a disincentive to individuals who wished to object to their data being collected and used.

CLEARVIEW'S APPEAL

Clearview appealed to the First-tier Tribunal against the ICO's decisions. In October 2023, the Tribunal upheld the appeal, finding that the ICO did not have jurisdiction to issue the enforcement and penalty notices, even though the processing related to the monitoring of behaviour of people in the UK. The Tribunal's reasoning was that it was beyond the material scope of the UK GDPR (being outside the scope of EU law) and was therefore not relevant processing for the purposes of Article 3 UK GDPR "*the activities of foreign governments fall outside the scope of Union law. It is not for one government to seek to bind or control the activities of another sovereign state*."

Clearview also asserted in its appeal that it had not breached UK data protection law, but the Tribunal focused on the jurisdiction aspects as a preliminary issue. If the ICO is granted permission to appeal, the more substantive question of whether Clearview breached UK data protection law is likely to come back into play.

HOW DOES THE UK GDPR APPLY TO NON-UK ENTITIES MONITORING UK DATA SUBJECTS?

The key provisions analysed by the Tribunal in reaching its decision were Article 3(2)(b) of the EU GDPR and the UK GDPR (these provide extraterritorial reach where there is processing related to the monitoring of behaviour of individuals in the EU/UK). The ICO considered that Clearview was within scope of UK data protection law because (i) processing of personal data of UK data subjects had been undertaken by a non-UK/EU established controller or processor (Clearview), (ii) the processing related to the monitoring of UK data subjects' behaviour (see next section), and (iii) the behaviour had taken place in the UK (or in the EU, prior to adoption of UK GDPR). The timing of the relevant events straddled the UK's withdrawal from the EU and therefore both the UK GDPR and the EU GDPR are referred to in the decisions.

PROCESSING, MONITORING BEHAVIOUR AND DATA PROTECTION ROLES

The Tribunal confirmed that Clearview's activities in providing its service involved the processing of personal data. These were split into:

- Activity 1: building, developing and maintaining the database (e.g. the scraping of images from the internet, storing the images, creating vectors from the images, indexing the images); and

- Activity 2: providing the service using the database (e.g. receipt of the client's probe images for the purposes of comparison with those held in the database, matching the vectors of the client's uploaded image against its database of vectors, returning search results to the client).

It also provided a detailed examination of what will constitute *behaviour* of a data subject, noting that the Clearview search results shared with the Tribunal showed aspects of data subject behaviour, such as relationship status, location, habits, occupations, associates and parental status.

The Tribunal also held that Clearview's activities constituted *monitoring* on the basis its clients are using the service not merely to identify people, but also with a view to taking decisions about them or predicting/analysing their behaviour, which constitutes monitoring of behaviour.

The Tribunal analysed the *data protection roles* applicable to the development of the database by Clearview and its use by Clearview clients, finding Clearview was a *controller* in relation to those activities underpinning the development of the database (Activity 1) and a *joint controller* when its service is used by its clients (Activity 2), as it determines the purposes of the processing (use in law enforcement / national security matters) and determines (with the client) the means of processing. It also held as a matter of law that Art (3)(2)(b) can apply to an organisation where the monitoring of behaviour is carried out by a third party and held, as a matter of fact, that the processing of data by Clearview was related to the monitoring of behaviour by Clearview's clients (sufficient for Article 3(2)(b) to apply in principle).

WHAT IS *BEHAVIOUR* IN THE CONTEXT OF AN IMAGE?

Every photographic image of a person will inevitably reveal something about them even, at the most basic level, that they had a photo taken or were smiling or "*simply that they were alive at the moment the photograph was taken*". The Tribunal's view was that the word *behaviour* indicates something more than simply being alive. "*We have concluded that a description of a person's behaviour will include a verb" … "in other words behaviour goes beyond mere identification or descriptive terms such as a person's height, hair colour, age, name or date of birth*". In the context of an image, a person's behaviour would include:

- where they are;
- what they're doing - including what they are saying / have said or what they have written as well as their employment or playing of sport or their pastime;
- who they associate with in terms of relationship;
- what they're holding or carrying;
- what they're wearing - including any items indicating cultural or religious background or belief.

WHAT DOES *MONITORING* MEAN FOR THE PURPOSES OF THE UK GDPR?

The Tribunal considered this will be intensely fact-specific, though monitoring can include a single incidence, based on the meaning of "track" (Recital 24 of the UK GDPR links determining monitoring of behaviour with ascertaining whether natural persons are tracked on the internet).

The Tribunal noted that the verb "to track" is capable of meaning either: (a) hunting or searching for someone to establish their position at a fixed point in time, and (b) the pursuit of a person over time, trailing them to identify where they are on more than one occasion. The sole act of identification by using the Clearview service would not be sufficient to constitute monitoring of the person's behaviour in their view. However, Clearview's clients are using the service to try to find out, not only who a person is, but also with a view to taking decisions about them, predicting or analysing the persons behaviour in order to apprehend them / gather evidence about what they have done or to prevent illegal activity. The Tribunal considered that continued monitoring of behaviour. The Tribunal held that Clearview's processing fell within Article 3(2)(b), as it was "related to" the monitoring carried out by their clients.

COMMENT

So far as we are aware, this is the first decision in the UK considering the data protection implications of providing an AI-powered image recognition service using a database compiled from harvested, publicly accessible images, including of UK data subjects.

The approaches of the Tribunal and the UK's data protection regulator indicate that monitoring of behaviour can have a broad interpretation when it comes to services incorporating databases of scraped images, with a potentially long jurisdictional reach. It will be interesting to see how this could play out for generative AI image-based services more generally.

This also comes at a time when:

- the ICO has begun 2024 with a consultation on generative AI models (to close on 1 March 2024). This first part of this consultation is to focus on the lawful basis on which generative AI models can be trained on web-scraped data (subsequent parts will examine how the purpose limitation principle applies when generative AI tools are developed and deployed, how to think about data accuracy in the context of these models and how innovators should be thinking about the rights of data subjects); and
- the UK government has just confirmed it will not proceed with its original proposal for a broad copyright exception for text and data mining (given concerns expressed by creators about the ability for AI innovators to profit from the work of human creators, particularly in the context of generative AI tools).

These two further developments are likely to have a material impact on the way in which AI developers can interact with personal data of UK residents and UK copyright materials, as well as for business models based on scraping publicly available data from the internet (to the extent this comprises personal data or works protected by copyright).

RELATED CAPABILITIES

- Data Privacy & Security

MEET THE TEAM

Anna Blest

London

anna.blest@bclplaw.com
+44 (0) 20 3400 4475

This material is not comprehensive, is for informational purposes only, and is not legal advice. Your use or receipt of this material does not create an attorney-client relationship between us. If you require legal advice, you should consult an attorney regarding your particular circumstances. The choice of a lawyer is an important decision and should not be based solely upon advertisements. This material may be “Attorney Advertising” under the ethics and professional rules of certain jurisdictions. For advertising purposes, St. Louis, Missouri, is designated BCLP’s principal office and Kathrine Dixon (kathrine.dixon@bclplaw.com) as the responsible attorney.