ICO Fines Clearview £7.5 Million for Data Protection Infringements

Date : July 14, 2022

We first issued this alert on 24 May 2022 and have updated it to reflect more recent developments.

Introduction

The UK Information Commissioner's Office (the ICO) fined Clearview AI Inc. (Clearview) £7,552,800 in May 2022 for data protection law infringements in using images of people for its AI product. Clearview collected images from the internet and from social media to create a global online database that could be used for facial recognition. The case is yet another reminder of the conflicts between AI & GDPR.

What's this all about?

Clearview provides a service that allows customers, including the police, to upload an image of a person to Clearview's app, which is then checked for a match against all the images in Clearview's 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 from where those images came from.

According to the ICO, Clearview collected 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 to create an online database. The affected individuals were however not informed that their images were being collected or used in this way. As the Information Commissioner, John Edwards, also put it, Clearview "[…] *not only enables identification of those people, but effectively monitors their behaviour and offers it as a commercial service [which] is unacceptable*." Because of the high number of UK internet and social media users, Clearview's database is, according to the ICO, likely to include a substantial amount of data from UK residents, which has been gathered without their knowledge.

Although (according to the ICO) Clearview no longer offers its services to UK organizations, Clearview has customers in other countries, so it is still using the personal data of UK residents.

What did the ICO decide?

The ICO decided that Clearview had infringed UK data protection law because it had:

- Failed to use the information of individuals in the UK in a way that is fair and transparent, given that individuals are not made aware or would not reasonably have expected their personal data to have been used in this way;
- Failed to have a lawful reason for collecting the personal data of individuals;
- Failed to have a process in place to stop the data being retained indefinitely;
- Failed to meet the higher data protection standards required for biometric data, which constitutes sensitive/special category personal data; and,
- Requested additional personal information, including photos, when asked by members of the public if they were on Clearview's database. This may have also acted as a disincentive to individuals who wished to object to their data being collected and used.

The ICO has also issued a so-called "enforcement notice" under which Clearview has been ordered to stop obtaining and using the personal data of UK residents that is publicly available on the internet, and to delete the data of UK residents from its systems. Clearview appealed the ICO's decision in July 2022.

AI under the Spotlight again

The ICO's latest action is part of a trend of global data protection enforcement actions that have been taken against Clearview. The ICO's action comes after a joint investigation between the ICO and the Office of the Australian Information Commissioner ("the OAIC"), which focused on Clearview's use of people's images, data

scraping from the internet and the use of biometric data for facial recognition. The investigation was also conducted under the Global Privacy Assembly's Global Cross-Border Enforcement Cooperation Arrangement and a Memorandum of Understanding between the ICO and the OAIC. There is background to this initial investigation here https://www.corderycompliance.com/clearview-to-close-oz-ops/. There is also civil action against Clearview in the US.

There is also civil action in the EU over AI algorithms. For example, drivers from the ride-hailing apps Uber and Ola Cabs started civil proceedings in Amsterdam in May over the enforcement of GDPR data subject rights and the role of algorithms in making management decisions. The drivers, supported by a pressure group and a union, have appealed an earlier court ruling to the Amsterdam Court of Appeal. The action has been brought by three UK based drivers and one based in Portugal. Uber say that drivers are not disciplined on a purely automated basis and that AI is there to support decisions but not to make them. It says that any decision which might affect a drivers' livelihood is subject to human review.

In April, the Hungarian DPA fined a bank in Budapest approximately £700,000 for carrying out automated decision-making and profiling based on an AI analysis of calls to its contact centre without a legal basis. In that case, the bank used AI to prioritise customer calls based on sentiment analysis.

Other Action against Clearview

As we have said, there has also been action against Clearview AI in other countries. In March the Italian the Italian Data Protection Authority (the Garante) fined Clearview €20m for GDPR violations. There is more information on that fine here https://www.corderycompliance.com/clearview-ai-italy-gdpr-fine/. Clearview was also fined €20m by the Greek DPA in July 2022. The Greek DPA also made similar stop processing and deletion orders.

In May the French DPA, CNIL, said that it may fine Clearview AI for failing to respond to an order to stop collecting images in France and to help people erase images scraped from the internet.

What are the takeaways?

The case clearly has implications for AI and shows again the conflict between the 'secret sauce' nature of AI and the need for transparency under GDPR. It also has wider implications for anyone using surveillance too – even something as simple as CCTV can cause compliance problems – we've looked at the general issues with CCTV here https://www.corderycompliance.com/client-alert-using-cctv-on-business-premises-dp-implications/ and specific cases with CCTV in the workplace in Germany here https://www.corderycompliance.com/german-cctv-fine/ and the use of Ring doorbells here https://www.corderycompliance.com/cctv-audio-breaches-dpa-rules/. In France the DPA has also taken action over surveillance by drone (see https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000042960768).

The case is also another reminder of GDPR's extra-territorial reach. In previous cases in the UK, Germany and Australia Clearview had argued that as a US corporation it was effectively only subject to US rules.

There are a number of more general lessons to be learned from this case too:

1. This case tells us that it is unwise to assume that because individuals' images/photos are publicly available on the internet or elsewhere that you are free to use them as you please, especially commercially. You will need to consider if legal restrictions, such as the UK GDPR, apply to the personal data captured in e.g. a photograph.
2. It may be best to undertake a Data Protection Impact Assessment (DPIA) to better determine the range of data protection issues that might apply and how to practically address them – if you are considering using biometrics or AI a DPIA will most likely be considered as obligatory.
3. Depending on the circumstances, you may wish to consider getting individuals to sign up to an image release waiver (to cover privacy and other issues). Bear in mind however that there can be issues with a consent-based approach under GDPR so this will also require careful planning.
4. Generally-speaking, when collecting personal data from individuals you should always consider being

upfront with them about what you will use their personal data for and consider putting in place a data retention plan and policy.
5. Bear in mind that compensation claims alleging data protection infringements against organizations continue to be on the rise.
6. Also be aware that under UK law there are various ways that an individual might try and prevent the commercial use of an image/photograph in which they appear, i.e. this is not an issue solely limited to UK GDPR considerations.

More Information

You can watch a film talking about this case and the legal aspects of AI here https://bit.ly/techlawai

There is more information about this and other data protection topics in Cordery's GDPR Navigator subscription service. GDPR Navigator includes short films, straightforward guidance, checklists and regular conference calls to help you comply. More details are at www.bit.ly/gdprnav.

We report about data protection issues here: https://www.corderycompliance.com/category/data-protection-privacy/.

The ICO's press release about the Clearview case can be found here https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2022/05/ico-fines-facial-recognition-database-company-clearview-ai-inc/.

For more about GDPR please also see our GDPR FAQs which can be found here: http://www.corderycompliance.com/eu-data-protection-regulation-faqs-3/and our Data Protection Glossary which can be found here: http://www.corderycompliance.com/?s=glossary.

For more information please contact André Bywater or Jonathan Armstrong who are commercial lawyers with Cordery in London where their focus is on compliance issues.

Jonathan Armstrong, Cordery, Lexis House, 30 Farringdon Street, London, EC4A 4HH
Office: +44 (0)207 075 1784
Jonathan.armstrong@corderycompliance.com

André Bywater, Cordery, Lexis House, 30 Farringd Street, London, EC4A 4HH
Office: +44 (0)207 075 1785
Andre.bywater@corderycompliance.com