Client Alert: Clearview AI ordered to close down Australian operations + provisional UK fine announced

Date : December 16, 2021

We first published this note on 4 November 2021 and have updated it with news of the UK's provisional fine

Introduction

There's a real focus at the moment on the issues with AI and compliance. A number of countries (and the EU) are looking at new laws but we have found that AI developers and those who buy their products often forget that they have obligations already under data protection laws including GDPR. There was a reminder of this at the start of this month after a joint investigation by regulators in the UK & Australia into Clearview AI and its facial recognition system. The Australian regulator has effectively closed down their Australian operations and ordered them to destroy the data they have on Australians. The UK regulator has announced a provisional fine for Clearview AI of £17m for GDPR violations. Both regulators have said that they are also looking into the police forces who used that technology to identify people in public places.

What was this about?

Clearview AI is a US based corporation which claims to use innovative AI technology to identify individuals including people wanted by law enforcement. They claim to have more than 3 billion images indexed in their database including people from outside the US. Some of their images have been scraped from social media although a number of social media operators including twitter, YouTube and Facebook have asked them to stop this practice. It is fair to say that their technology, its use, and some of its customers, have been controversial. Proceedings have been issued against them and a number of data protection authorities have received complaints.

What was this investigation about?

As we've said previously data protection authorities (DPAs) have become much more interested in AI recently. In Spain and Italy there has been a long-running investigation into AI in food delivery with two fines handed down earlier this year (see https://bit.ly/aiitfines). In August 2020, the Hamburg DPA issued an administrative order against Clearview AI instructing them to provide answers to questions they had asked. In July 2020, the UK DPA (the ICO) and the Australian DPA (the OAIC) also launched a joint investigation into Clearview AI.

The ICO/OAIC investigation found that Clearview AI had behaved unlawfully in part because its data processing was not transparent. Transparency is a key theme of GDPR – more than €1bn worth of GDPR fines relate to the breach of the transparency obligations under GDPR. We've written before about the transparency obligation and how it impacts AI here https://bit.ly/gdpraistuff.

OAIC findings

The OAIC found that Clearview AI breached Australian data protection law by:

- collecting Australians' sensitive information without consent
- collecting personal information by unfair means
- not taking reasonable steps to notify individuals of the collection of personal information
- not taking reasonable steps to ensure that personal information it disclosed was accurate, having regard to the purpose of disclosure; and
- not taking reasonable steps to implement practices, procedures and systems to ensure compliance with the Australian Privacy Principles.

The OAIC ordered Clearview AI to cease collecting facial images and biometric templates from individuals in Australia, and to destroy existing images and templates collected from Australia. On 15 December 2021, the OAIC

also said that Australia's Federal Police Force breached data protection rules when using Clearview.

ICO provisional findings

On 29 November 2021, the ICO announced its provisional intent to impose a potential fine of just over £17m on Clearview AI. In addition, the ICO has issued a provisional notice to stop further processing of the personal data of people in the UK and to delete the data it has already obtained. As we have said before, often orders to stop processing and delete data can be more consequential than a fine. In this case, the ICO has followed the practice of some other DPAs including Italy, of issuing a fine and a prohibition on processing.

In many respects, the ICO's provisional findings are similar to those of the OAIC. The ICO's provisional view is that Clearview AI breached UK Data Protection law by:

- failing to process the information of people in the UK in a way they are likely to expect or that is fair
- failing to have a process in place to stop the data being retained indefinitely
- failing to have a lawful reason for collecting the information
- failing to meet the higher data protection standards required for biometric data (classed as 'special category data' under GDPR and UK GDPR)
- failing to inform people in the UK about what is happening to their data; and
- asking for additional personal information, including photos, which may have acted as a disincentive to individuals who wish to object to their data being processed.

Like in Australia, the ICO understands that Clearview AI was offered in the UK on a free trial basis but the trials were discontinued. The ICO says it does not believe that Clearview AI services are currently being offered in the UK.

There is still a way to go however before the ICO's fine is confirmed. The ICO has said that it expects to make a final decision by mid-2022 but we know that timelines like this have been put back in other cases.

What about the EU?

As we have said, the Hamburg DPA has already taken preliminary enforcement action. It followed up its initial enforcement action in January 2021 by issuing a draft order to Clearview AI seeking the deletion of data related to one complainant.

Clearview AI's practices have also been debated by the EDPB in 2020. In June 2020, the EDPB wrote to a number of MEPs expressing its concern although enforcement action will be taken by individual DPAs in the EU rather than by the EDPB itself.

In February 2021, the Swedish DPA found that the police in Sweden had behaved unlawfully when using Clearview AI. They were fined SEK 2,500,000 (around €250,000) and also ordered to put remediations in place including extra training.

On 16 December 2021, the French Data Protection Authority, CNIL, ordered Clearview AI to stop collecting and using photographs and videos of people in France and ordered them to delete any data that they already had within two months. CNIL also told Clearview AI that they must help people exercise their GDPR right to have data erased.

Extra Territoriality

The case also shows the extra territorial nature of data protection law. GDPR has some fairly detailed provisions on territorial scope in GDPR Art.3, which allow regulators within the EU (and currently the UK) to take action in a number of circumstances including where a company outside the EU monitors the behaviour of individuals within

the EU. It is relatively common for regulators to have extra territorial ambitions and this case shows that both the Australian regulator and the UK regulator felt comfortable investigating a US based corporation. The DPA in Hamburg also reached similar conclusions.

We have had quite a few non-EU operations fined under GDPR and it is important to remember that if GDPR applies to your organisation and you are outside the EU, you might have to put in place additional protections as well. In May 2021, the Netherlands DPA fined Locatefamily €525k for failure to appoint a data protection representative in the EU. You can read more about that case here https://www.corderycompliance.com/locatefamily-fined-by-ap/

In representations to the OAIC Clearview argued that it was not subject to Australian law because it was based in the US and only carried out business in that country. It also said that none of its business related to Australian individuals. The OAIC investigation found however that Clearview had offered free trials to Australian Federal Police and a number of State-based police forces. In the trials, the tool had been used to identify victims and suspects in investigations and it also put forward images of children. Clearview said that that activity had stopped in March 2020. The OAIC said however that it was satisfied that during the trial period, Clearview had carried on business in Australia. It also said that Clearview continued to collect the facial images of Australians.

Facebook's Response

It does seem that a number of organisations have become more and more concerned about the use of AI and the ethical issues involved. Earlier this month Facebook (and its newly named parent company Meta) announced that it would delete more than a billion facial recognition templates and that it would also stop automatically recognising the identities of individuals captured in photos and videos.

It has been reported that IBM, Microsoft and Amazon have also suspended sales of facial recognition technology to police forces. Facebook agreed a $5bn privacy settlement with the US Federal Trade Commission, in part because of its use of facial recognition. It also agreed a $650m settlement relating to allegations that Facebook had violated Illinois biometric laws.

What does this mean?

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).

What happens next?

It is likely that this case will continue. Firstly, we can expect Clearview AI to challenge the regulators' findings. They may well try and challenge the jurisdiction of both the OAIC and the ICO. They are likely to make representations on the ICO's draft provisional findings and we can expect an appeal if the provisional findings are confirmed.

Clearview has already appealed the OAIC decision and a lawyer for the company told MLex (https://mlexmarketinsight.com/) that Clearview was already considering an appeal against the ICO's provisional findings. How exactly it might do that before a fine is confirmed remains to be seen.

Since both the ICO and OAIC have determined that data has been processed unlawfully, we can expect litigation. We have talked before about the rise in data protection litigation in Europe and, despite the doors closed by the Supreme Court Judgment in Lloyd v Google LLC (see here

https://www.corderycompliance.com/lloyd-v-google-ruling/), we can still expect claimants to try. There has been litigation against Clearview AI in the US and litigation in the UK seems likely.

We can also expect additional activity at an EU level including further action by the Hamburg DPA and others.

There is clear political concern about this type of activity. For example, the new German coalition Government has been reported as being in favour of the EU's proposed Artificial Intelligence Act which seeks to outlaw some of the activity that Clearview AI were involved with.

All of these cases also show public concern about surveillance and monitoring which is likely to be a feature of more significant cases too.

More Information

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.

For anyone who's interested the Australian announcement is here https://bit.ly/3bBDJ6R and the UK announcement here https://bit.ly/3k0Ar1N. The ICO's announcement of the provisional fine is here https://bit.ly/3G5XD7r

For more information please contact Jonathan Armstrong or André Bywater who are 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