THE INFORMATION COMMISSIONER'S OFFICE ISSUES NOTICE OF INTENT TO FINE CLEARVIEW AI INC £17M

10 / 12 / 2021

The Information Commissioner's Office (ICO) has announced its intent to impose a fine of just over £17 million on Clearview AI Inc (CI) a company that describes itself as the 'World's Largest Facial Network'. In addition, the ICO has issued a provisional notice ordering CI to stop further processing of the personal data of UK citizens. It has also required Clearview to delete all UK citizen personal information.

The ICO had conducted a joint investigation with the Office of the Australian Data Protection Commissioner (OAIC). This was conducted in accordance with the Australian Privacy Act 1988 and the UK Data Protection Act 2018.

CI develops facial recognition software, widely used by US law enforcement agencies and private companies. It is alleged that CI 'scrapes ' images from the Internet and processes biometric data to identify people.

The collection of publicly available personal information from the internet is known as 'data scraping.' This typically involves the use of technology to 'scrape' the information from the internet.

The problem with obtaining personal information in this manner is that it is very difficult if not impossible to comply with data protection law. For example Article 13 of the General Data Protection Regulation (GDPR) lists the information to be provided where personal data are collected from a data subject:

- The identity and contact details of the data controller.
- The contact details of the data protection officer.
- The purpose of the processing and legal basis for processing.
- Details of any transfer to a third country.
- Period for which the data will be stored.
- Data subjects rights.
- Right to lodge a complaint a supervisory authority.

It is the view of the ICO that the images in CI's database are likely to include the data of a substantial number of people from the UK and may have been gathered without people's knowledge from publicly available information online, including social media platforms. The ICO also understands that the service provided by CI was used on a free trial basis by a number of UK law enforcement agencies, but that this trial was discontinued and CI's services are no longer being offered in the UK.

It is understood that the Clearview database contains over 10 billion images.

The ICO has said that CI's facial recognition app allows users to upload an image of an individual's face and match it to photos of that person collected from the internet and stored in CI's database.

The ICO's preliminary view is that CI appears to have failed to comply with UK data protection laws in several ways including:

- 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 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.

The ICO's notice comes after a 2020 investigation by the European Data Protection Board (EDPB) concluded that Clearview's facial recognition software does not meet the conditions set out in the EU's Law Enforcement Directive.

The data protection authorities in Austria, France, Greece and Italy are also investigating CI's data processing.

CI now has the opportunity to make representations in respect of the Commissioner's Notice of Intent and Preliminary Enforcement Notice.

Conclusion

Organisations which intentionally 'scrape' personal information from the Internet must be aware that where an individual can be identified from the information collected data protection laws are triggered.

Organisations must also be aware that personal information that is publicly available cannot be used for direct marketing purposes without the individual's consent. The ICO issues more fines for breaches of the Privacy and Electronic Communications (EC Directive) Regulations 2003 than any other data protection breaches.

Organisations should also be aware that 'scraping' facial images of individuals for identification purposes is very likely to be considered 'biometric data.' Article 9(1) GDPR includes in the list of special categories of data biometric data for the purpose of uniquely identifying a natural person.

It is clear that many data protection authorities consider such breaches of data protection laws to be very serious.