Clearview AI Beats UK GDPR Fine Over Facial Recognition, ICO Deemed Out of Its Jurisdiction

A UK GDPR fine that would have cost Clearview AI the equivalent of $9.1 million has been overturned, as an appeals court found that lead regulator ICO was outside of its jurisdiction in penalizing the foreign facial recognition firm.

The £7.5 million fine has been erased as the court determined that the UK regulator cannot make enforcement decisions based on how foreign law enforcement agencies use the data of British citizens

Facial recognition firm lets fines, scraped photos sit as legal challenges proceed
The controversial facial recognition firm has been chased out of numerous major markets at this point, but the UK decision demonstrates why it has tended to avoid paying fines and hang on to the collections of pictures it scraped. Things still do not bode well for the company in the EU (not to mention Australia, Canada, and certain US states), but the UK GDPR fine reversal indicates that it may at least get out of seemingly devastating financial trouble.

The UK court decision appears to hinge on the fact that Clearview AI has, since forced to by a settlement in 2020, only accepted legitimate law enforcement agencies as clients. The court determined that ICO does have the power to act against foreign companies that scrape the data of UK citizens, but that an exception had to be made in this case as the only impact would be to foreign law enforcement agencies (primarily in US states that have not taken action against Clearview AI or use of facial recognition technology for these purposes, as well as some Latin American countries).

The UK GDPR fine thus would have been seen as “binding or controlling” the activities of another sovereign state’s agencies. ICO has said that it is “carefully considering” the precedent set by the fine but will continue to pursue regulatory action against scraping that does not fall into this relatively narrow set of circumstances.

The UK GDPR fine decision raises questions about the firm’s other legal appeals, particularly in the EU. It faces similar large fines from France, Italy and Greece, totalling over $60 million (including overdue penalties it has been racking up in France since May of this year). The company is thought to have raised about $38 million from investors to date, and given its increasingly narrow geographic range of business opportunities it could easily end up underwater if it actually paid these amounts. Thus far it has been dodging them as it no longer does business in the regions that it has been fined in.

UK GDPR fine creates precedent for foreign national security and law enforcement agencies
The regulations the UK ICO operates under are rooted in the EU’s General Data Protection Regulation system, but vary in some ways since the country broke off from the bloc. The UK court found that Clearview AI met the definition of a joint controller for data processing purposes, subjecting it to consent requirements, and that the processing involved the behavior of data subjects (both conditions essentially copied from GDPR terms). The distinction about exclusive use by foreign government agencies is found in the terms of the UK’s Data Protection Act 2018, meaning that the facial recognition firm may not be able to use this same tack to get off the hook for pending

fines in other countries. Had ICO brought its claim against Clearview AI under the rules of the UK GDPR rather than the Data Protection Act, this appeal may not have been successful.

Even if it cannot wiggle out as it did with the UK GDPR fine, the controversial facial recognition firm can continue to beat its EU fines by simply refusing to pay them (assuming it never plans to return to the bloc to do business). France has recently reached out to the US Federal Trade Commission about compelling the company to pay its mounting fines (where it continues to rack up millions of euros in late fees), but nothing has appeared to come of it as of yet.

EU law has some added layers working against Clearview AI, via the European Data Protection Board (EDPB) which has published guidance stating that facial recognition firms serving law enforcement clients do not receive exceptions to regulatory terms. The EDPB and the European Data Protection Supervisor have also called for a bloc-wide ban on mass indiscriminate processing of data for law enforcement purposes, citing the sort of scraping that Clearview AI does as a specific example of what should be clearly outlawed. The upcoming EU AI Act contains a clause of this nature, though it remains in draft status at present.

The company remains able to offer its facial recognition services in the US, where it is based, so long as it rigorously avoids collecting the biometric data of residents of Illinois.