A Clear View of the Risks of Indiscriminate Digital Facial Recognition

Francesca Allport
Solicitor, Wedlake Bell LLP

Alexander Dittel
Partner in Technology, Wedlake Bell LLP

Biometric data; Data protection; Facial recognition software; Fines; Law enforcement; Surveillance

Clearview AI Inc was fined over £7.5 million by the Information Commissioner's Office (ICO) for the processing of biometric data of individuals in the UK. According to the UK Information Commissioner, Clearview "effectively monitors their behaviour and offers it as a commercial service".[1] The fine was reduced from the provisional £17 million proposed back in November 2021.[2]

This does not come as a surprise following the ICO's joint investigation with the Office of the Australian Information Commissioner which issued its determination in November 2021.[3] Similarly, in Canada, Clearview was ordered to stop breaching federal and provincial privacy laws by scraping images from the internet without permission. In Sweden, Clearview was fined €250,000 for its unlawful processing of facial images without individuals' knowledge or consent.[4] In Italy, Clearview was fined €20m for processing biometric and geolocation information without an appropriate legal basis, given the "legitimate interest of the US-based company does not qualify as such".[5]

In 2019, the Indiana State Police in the US, which according to sources was Clearview's first paying customer, used the tool to identify a shooter who had no driver's licence and had not been arrested as an adult. The police claimed that without that app the perpetrator would not be found. Described as a "superior" app, Clearview offered a much larger database than alternative services and it did not require photos of people looking straight at the camera. In fact, it can allegedly still return valid results if the face is partially covered from the nose down. Acknowledging "there's always going to be a community of bad people who will misuse it", Clearview's founder Mr Ton-That holds the belief that "this is the best use of the technology".[6]

To put this into context, the Facial Recognition Technology (FRT) industry is projected to reach $12.67 billion by 2028 from $5.01 billion in 2021 and is expected to grow 14.2% from 2021 to 2028.[7] FRT has become prevalent in our day to day lives from how we unlock our device to going through border control at the airport. However, as the technology evolves to become widespread in our personal lives, law enforcement is cognisant of the potential to use FRT for the greater good. FRT could help search for persons in police watch lists, monitor a suspect's movements in the public space or identify perpetrators of illegal activity online.

However, it is very difficult to reconcile the way Clearview operates with the General Data Protection Regulation (GDPR).[8] Indiscriminate scraping of images from the web for purposes which may have a direct impact on individuals without their knowledge will likely be unlawful. Clearview is directly liable because it processes data for its own purposes as a "controller" in order to build its database. It is not hiding behind the "processor" status like so many other service providers who claim to act strictly on client instructions.

The Clearview AI case reminds us of the risks of indiscriminate use of FRT and perhaps where we wish the line to be drawn. We see a flow of responses to FRT at national and international level, to name a few, California's ban of FRT in law enforcement,[9] cases such as *R. (on the application of Bridges) v Chief Constable of South Wales Police*,[10] ICO guidance on the use of FRT in

[1] ICO fines facial recognition database company Clearview AI Inc more than £7.5m and orders UK data to be deleted; available at *https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2022/05/ico-fines-facial-recognition-database-company-clearview-ai-inc/*.
[2] ICO issues provisional view to fine Clearview AI Inc over £17 million; available at *https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2021/11/ico-issues-provisional-view-to-fine-clearview-ai-inc-over-17-million/*.
[3] Clearview AI breached Australians' privacy: available at *https://www.oaic.gov.au/updates/news-and-media/clearview-ai-breached-australians-privacy*.
[4] Swedish DPA: Police unlawfully used facial recognition app: available at *https://edpb.europa.eu/news/national-news/2021/swedish-dpa-police-unlawfully-used-facial-recognition-app_en*.
[5] Facial recognition: Italian SA fines Clearview AI EUR 20 million; available at *https://edpb.europa.eu/news/national-news/2022/facial-recognition-italian-sa-fines-clearview-ai-eur-20-million_en*.
[6] The Secretive Company That Might End Privacy as We Know It, NY Times, 18 January 2020; available at *https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html*.
[7] Facial Recognition Market Size Worth $12.67Bn, Globally, by 2028 at 14.2% CAGR - Exclusive Report by The Insight Partners; available at *https://www.prnewswire.com/news-releases/facial-recognition-market-size-worth-12-67bn-globally-by-2028-at-14-2-cagr—exclusive-report-by-the-insight-partners-301489784.html*.
[8] Regulation 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data [2016] OJ L119/1.
[9] Three-year ban on police use of facial recognition technology in California to start in the new year; available at *https://www.sandiegouniontribune.com/news/public-safety/story/2019-12-20/3-year-ban-on-police-use-of-facial-recognition-technology-in-california-to-start-in-the-new-year#:~:text=Assembly%20Bill%201215%20prohibits%20officers,It%20will%20take%20effect%20Jan*.
[10] *R. (on the application of Bridges) v Chief Constable of South Wales Police* [2020] EWCA Civ 1058; [2020] 1 W.L.R. 5037.

public spaces,[11] and the United Nations report on the right to privacy in the digital age.[12] More recently, the European Data Protection Board (EDPB) issued its guidelines on the use of facial recognition technology in the area of law enforcement.[13] There is consensus that this fast-growing sector is in need of regulation to tackle high risk application of FRT.

Biometric data

Clearview relies on FRT which is described by the EDPB as "a probabilistic technology that can automatically recognise individuals based on his/her face in order to authenticate or identify them".[14] FRT algorithms detect and analyse faces and create unique digital biometric templates that are used to match and identify individuals in photos, videos and real time.

More broadly, FRT falls into the category of biometric technology. Biometric information is of an intrinsically private nature and more permanent than other data, and can be used to uniquely identify an individual in a range of different contexts.[15] Biometric technology includes "all automated processes used to recognise an individual by quantifying physical, physiological or behavioural characteristics or biometric data".[16] Unlike an address or a telephone number, it is impossible to change one's unique characteristics. If used as a password or cryptographic key, their publication would lead to the data being compromised. The processing of biometric data is generally prohibited under the GDPR, unless certain conditions are met.

Particularly difficult to justify is the use of FRT for indiscriminate monitoring of individuals in public spaces without a sufficiently targeted approach. The Data Protection Act 2018 which implements the Law Enforcement Directive[17] requires that the processing of biometric data shall only be allowed where strictly necessary for defined law enforcement purposes and subject to appropriate safeguards for the rights and freedoms of the data subject. Strictly necessary, in this instance, means that the interference with fundamental rights is limited to what is absolutely necessary.[18]

The deployment of FRT for indiscriminate application in the private sector is even more difficult. For example, a Dutch supermarket who connected FRT to cameras at the store's entrances to protect its customers and staff along with preventing shoplifting was issued a formal warning. The Dutch data protection authority stated:

> "It's unacceptable for this supermarket—or any other store in the Netherlands—to just start using facial recognition technology … use of such technology outside of the home is banned in nearly all cases. And that's for good reason."[19]

About Clearview AI

Originally called Smartcheckr, the company changed its name to Clearview at the end of 2017 as it was positioning its service in the surveillance market.

According to the ICO, the customer uploads a probe image. The Clearview tool then derives facial vectors from that image which are compared against the facial vectors drawn from the images in its database. The search result includes images with similar characteristics together with their URLs. The service does not provide any opinions as to the identity, or attributes, of the individual shown in the probe image.[20]

Clearview's database is an important asset developed and maintained by scraping images from the public-facing internet. The images, metadata, URLs, facial vectors and geolocation data are collected by Clearview at its own instigation, without client instruction or preferences. The ICO observed that the "images that are disclosive of information about a UK resident's behaviour are more likely than not to relate to their behaviour in the UK".[21] The facial vectors derived from images constitute special category data. This means that Clearview's FRT must comply with the Data Protection Act 2018 and the UK GDPR.

The company explained that it only uses publicly available images. For example, if one changes their Facebook privacy setting so that search engines can no longer link to one's profile, the images from that profile will not end up in Clearview's database.[22] However, many

[11] Information Commissioner's Opinion: The use of live facial recognition technology in public places 18 June 2021; available at *https://ico.org.uk/media/2619985/ico-opinion-the-use-of-lfr-in-public-places-20210618.pdf*.
[12] United Nations High Commissioner for Human Rights' report on the right to privacy in the digital age; available at *https://www.ohchr.org/en/calls-for-input/report-right-privacy-digital-age*.
[13] Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement Version 1.0 Adopted on 12 May 2022; available at *https://edpb.europa.eu/our-work-tools/documents/public-consultations/2022/guidelines-052022-use-facial-recognition_en*.
[14] Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement Version 1.0 Adopted on 12 May 2022; available at *https://edpb.europa.eu/our-work-tools/documents/public-consultations/2022/guidelines-052022-use-facial-recognition_en*.
[15] Information Commissioner's Opinion: The use of live facial recognition technology in public places 18 June 2021; available at *https://ico.org.uk/media/2619985/ico-opinion-the-use-of-lfr-in-public-places-20210618.pdf*.
[16] Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement Version 1.0 Adopted on 12 May 2022; available at *https://edpb.europa.eu/our-work-tools/documents/public-consultations/2022/guidelines-052022-use-facial-recognition_en*.
[17] Directive 2016/680 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA [2016] OJ L119/89.
[18] As per CJEU case law.
[19] Dutch DPA issues Formal Warning to a Supermarket for its use of Facial Recognition Technology | European Data Protection Board (europa.eu); available at *https://edpb.europa.eu/news/national-news/2021/dutch-dpa-issues-formal-warning-supermarket-its-use-facial-recognition_en*.
[20] Clearview AI Inc. Monetary Penalty Notice, ICO; available at *https://ico.org.uk/media/action-weve-taken/mpns/4020436/clearview-ai-inc-mpn-2022051 8.pdf*.
[21] Clearview AI, Inc. Monetary Penalty Notice, ICO; available at *https://ico.org.uk/media/action-weve-taken/mpns/4020436/clearview-ai-inc-mpn-2022051 8.pdf*.
[22] The Secretive Company That Might End Privacy as We Know It, NY Times, 18 January 2020; available at *https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html*.

Facebook users remain naïve about the perils of the world wide web and are unsuspecting enough not to take advantage of such features.

With Clearview, searching someone by face could become as easy as using a search engine. One could take photos of strangers and find out about their relationships or even addresses with a few clicks: "it would herald the end of public anonymity".[23] Under the GDPR, Clearview must comply with the transparency, lawful basis, limited data retention and strict rules about justifying the processing of biometric data. The company failed on all counts.

In the US, the company hired a law firm to opine on the legality of the service. The legal memo provided allegedly helped many US police departments to make up their minds to purchase the service. However, it transpired that the service violates even US laws. The Illinois Biometric Information Privacy Act (BIPA) was invoked by the American Civil Liberties Union (ACLU) against Clearview's indiscriminate processing of biometric data without peoples' consent. Under the settlement with the ACLU,[24] Clearview agreed to only sell its "bias-free" FRT algorithm without the database to commercial entities and to only offer its database to law enforcement agencies outside of Illinois.[25]

Clearview would likely be able to lawfully sell its FRT technology without the database in the UK. An interesting questions arises whether an algorithm trained on data obtained unlawfully can lawfully be used without that data. Whilst such draconian rule seems unlikely, we do not know how in an AI-saturated world in near future case law and regulatory practice might develop.

Nevertheless, this somewhat steep learning curve did little to dislodge Clearview leadership's aspiration to use its technology for the greater good. Recently, Clearview explained how its technology is used by a visitor management software provider or that it could be used in large bank transactions to verify the account holder's identity. According to the founder, "the potential of facial recognition technology to make our communities safer and commerce secure is just beginning to be realized".[26]

Risks of FRT

While acknowledging the benefits of FRT, the United Nations High Commissioner for Human Rights' report on the right to privacy in the digital age (the UN report),[27] highlights the negative, and even catastrophic, effects on human rights of remote biometric recognition, predictive biometrics, people analytics and other artificial intelligence (AI).

Mass surveillance by FRT-enhanced CCTV undermines the ability of individuals to go about their lives unobserved and has a chilling effect on freedom of expression, peaceful assembly and association. While notorious in some countries, this is banned under the draft AI Act[28] and would likely be unlawful in the UK. The UN report calls for a moratorium on this surveillance, at least until compliance can be safely established. The intrusion by FRT in public spaces is greater than simple observation or photograph because of the large-scale and automated processing of data, often undertaken without reasonable suspicion and arbitrarily. Any probabilistic and opaque processing of data that triggers state intervention, such as searches or questioning, is particularly invasive, despite human judgement being equally unreliable.

The European Data Protection Supervisor called for a ban of processing in relation to: (1) remote biometric identification of individuals in public spaces; (2) AI-supported facial recognition systems categorising individuals based on their ethnicity, gender, political or sexual orientation and similar grounds; (3) use of facial recognition or similar technologies, to infer emotions of a natural person; and (4) processing of personal data in a law-enforcement context that would rely on a database populated by collection of personal data on a mass scale and in an indiscriminate way, e.g. by "scraping" photographs and facial pictures accessible online.[29] The processing of biometric data also involves the risk of abuse by the relevant authorities as a result of unlawful access or use of the personal data or a security breach.

Under *Bridges*, the greater the human rights interference, the more specific the lawful basis of data processing must be. According to the EDPB, for most applications of FRT in the law enforcement context, a specific law precisely describing the application and the conditions for the use of FRT will be required for it to be lawful. Such law must define a legitimate objective. According to the EDPB, "an objective of general interest—however fundamental it may be—does not, in itself, justify a limitation to a fundamental right". Furthermore, the use of FRT must not exceed the limits of what is appropriate and necessary in order to achieve those objectives.

The EDPB guidance gives various examples of proportionate and necessary application of FRT. This includes, for example, the use of e-gates at airports or even retrospective analysis of images using FRT and comparing against the Police database of suspects and former convicts. This appears similar to the Clearview

[23] As above.
[24] Settlement Agreement; available at *https://regmedia.co.uk/2022/05/09/aclu_clearview_settlement.pdf*.
[25] Clearview AI promises not to sell face-recognition database to most US businesses, The Register; available at *https://www.theregister.com/2022/05/10/clearview_ai_alcu/*.
[26] Clearview AI wants its facial-recognition tech in banks, schools, etc, The Register; available at *https://www.theregister.com/2022/05/25/clearview_banks_schools/*.
[27] A/HRC/48/31: The right to privacy in the digital age—Report of the United Nations High Commissioner for Human Rights; available at *https://www.ohchr.org/en/documents/thematic-reports/ahrc4831-right-privacy-digital-age-report-united-nations-high*.
[28] Proposal for a Regulation laying down harmonised rules on artificial intelligence; available at *https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-laying-down-harmonised-rules-artificial-intelligence*.
[29] EDPB & EDPS call for ban on use of AI for automated recognition of human features in publicly accessible spaces, and some other uses of AI that can lead to unfair discrimination; available at *https://edpb.europa.eu/news/news/2021/edpb-edps-call-ban-use-ai-automated-recognition-human-features-publicly-accessible_en#:~:text=Taking%20into%20account%20the%20extremely,of%20faces%2C%20gait%2C%20fingerprints%2C*.

service. However, the Police database is created lawfully, as opposed to the Clearview database which was created in a breach of the GDPR and cannot be lawfully used.

The difficulties in applying FRT do not end with indiscriminate deployment of the technology. According to the UN report, even a relatively uncontroversial discrete use of FRT for identity verification may be disproportionate if no alternative is provided to the service user.

Conclusion

The lawfulness of FRT will hinge on evolving laws and regulatory practice, which must remain aligned with societal acceptance.[30] While the society in the UK would likely strongly oppose the type of FRT developed by Clearview, we can also perceive undeniable benefits of its application in the law enforcement sector subject to strong safeguards and targeted application. The UK Government seems to agree.

As part of the data reform the UK Government claims that:

> "Technologies such as DNA and fingerprint analysis, and, increasingly, facial image recognition, are important public safety tools for the police. The public rightly expects the police to use these tools within a framework that ensures use is fair, transparent and proportionate."

At the same time, the consultation highlighted that "adoption of all new major data-driven operational technologies"[31] seems challenging for the police. Its desire to move fast on this is demonstrated by the fact that the UK Government did not find it necessary to discuss with the Biometrics and Surveillance Camera Commissioner Fraser Sampson the then upcoming consultation about the transfer of his statutory functions to the ICO,[32] in a bid to simplify the use of biometrics in law enforcement.

With a growing population and the need for the effective resolution by governments of issues that arise at large scale, surveillance is ever more popular around the world. Perhaps the UK is also about to shake off its natural resistance to services such as Clearview. This news will be welcomed by the surveillance industry which is set to gain significantly by a relaxation of the rules. Thankfully, privacy advocates will likely also have their voice heard on this matter.

[30] Response by the Biometrics and Surveillance Camera Commissioner to DCMS data reform; available at *https://www.gov.uk/government/publications/data-a-new-direction-commissioners-response/dcms-consultation-data-a-new-direction-response-by-the-biometrics-and-surveillance-camera-commissioner-accessible-version*.
[31] Data: a new direction - government response to consultation Updated 17 June 2022; available at *https://www.gov.uk/government/consultations/data-a-new-direction/outcome/data-a-new-direction-government-response-to-consultation*.
[32] DCMS consultation: "Data: a new direction": response by the Biometrics and Surveillance Camera Commissioner; available at *https://www.gov.uk/government/publications/data-a-new-direction-commissioners-response/dcms-consultation-data-a-new-direction-response-by-the-biometrics-and-surveillance-camera-commissioner-accessible-version*.