“Walking bar codes”, Swedish Police and the use of Facial Recognition Technology

Published 30 April 2021

The Dutch Data Protection Authority (“**DPA**”) issued a formal warning to a Dutch supermarket for use of facial recognition technology (“**FRT**”) in its stores. The supermarket claimed to be using FRT to protect its customers and employees, and to prevent shoplifting. However, the deputy chair of the DPA warned that FRT makes us all “*walking bar codes*” and highlighted the need for customers to give explicit consent in the absence of any necessity for authentication or security purposes.

Supermarket Scanning

The Dutch supermarket, which is unnamed in the DPA’s decision, undertook scanning of the faces of all individuals who entered the store and cross-referenced it against a database of people who had been banned from entering stores. It is noted that the faces of people who had not been banned were deleted after only a few seconds.

The supermarket’s use of FRT was reported in the Dutch media and, on 6 December 2019, the DPA requested information from the owner of the supermarket. The FRT was disabled two days later but the owner of the supermarket indicated to the DPA that he wished to reinstate its use.

However, the DPA issued a warning that FRT could not be used in the supermarket and noted that the mere fact that individuals had been told that FRT was in use, and still entered into the supermarket, could not be taken as the giving of explicit consent. Although the supermarket had claimed that FRT was in use for security purposes, the DPA did not agree. The bar for use of FRT for security purposes is high, with the DPA citing its use for the security of a nuclear power plant as an example of where it is justified. It expressly drew a distinction between the preventing of shoplifting being of a “*completely different magnitude than preventing a nuclear disaster*”.

What is FRT and why the controversy?

FRT works by pinpointing and measuring facial features from images and using algorithms to estimate the degree of similarity between two faces. The technology can be used retrospectively or live and can be fully automated.

FRT has long been complained about by privacy campaigners given the potential for it to breach individuals’ human rights (to respect for private and family life), restrict liberty (where used by law enforcement), or cause bias and discrimination given the use of characteristics such as gender and ethnicity. It is also considered controversial because of the risk of being used to extract additional, unnecessary personal data associated with an individual, such as other photos, social media profiles, online behaviours, and travel patterns.

In some circumstances, FRT has now been banned, as is the case California where it is now prohibited to use FRT as part of law enforcement. In January 2020, the EU toyed with the idea of banning the use of FRT in public places, but it went no further than that. Notably, however, during the George Floyd protests in May 2020 in the USA, use of FRT by city government was apparently banned in Boston, Massachusetts.

Notwithstanding the risks and controversy, FRT continues to be widely utilised, such as on smartphones and in robotics. However, it is worth noting that when used for identification purposes, FRT will likely be considered a type of biometric data, and thus categorised as special category data under the GDPR. Where FRT meets the definition of biometric data under the GDPR, it cannot be processed lawfully unless the Article 6 requirements are met, and one of the Article 9 processing conditions applies (such as “explicit consent” of the individual, or “substantial public interest”).

Swedish Police

In another recent FRT decision, the Swedish DPA found that the Swedish Police Authority had processed personal data in breach of the Swedish Criminal Data Act, when utilising Clearview AI to identify individuals. The Swedish DPA’s investigation revealed that the Swedish Police had used Clearview AI on a number of occasions, and had unlawfully processed biometric data for facial recognition as well as having failed to conduct a data protection impact assessment which was required.

An administrative fine of SEK 2,500,000 (approximately EUR 250,000) was imposed on the Swedish Police for infringements of the Criminal Data Act. To add salt to the Swedish Police’s wounds, they were ordered to inform all data subjects whose data has been disclosed to Clearview AI, where confidentiality rules allowed it. They were also ordered to ensure, to the

extent possible, that any personal data transferred to Clearview AI was erased.

Conclusion

There is a discrepancy between the regulatory regime governing the use of FRT in law enforcement and in the private sector, as is evidenced by the stricter decision against the Swedish Police versus the Dutch supermarket. Both the supermarket and the Police had utilised the technology, but only one party was fined, and only one party was ordered to notify data subjects. More widely, we are starting to see a trend amongst regulators to impose an obligation on controllers to notify data subjects of breaches of the GDPR, even where a risk based analysis by that controller has concluded that the Article 34 GDPR threshold has not been met.

Authors