


Privacy implications of facial recognition technology (FRT) in retail security

22 July 2025  Saara Leino and Francis Katamba

Facial recognition technology (FRT) is a type of biometric technology that identifies or verifies a person by analysing their facial features. It works by capturing an image or video of a face and converting it into a digital format, creating a unique facial signature. This signature can then be compared with stored data to confirm someone's identity.

While it is already used in areas such as law enforcement, workplace attendance, and unlocking devices, recent developments mean it can now also be used to detect emotions or behaviours — a trend that has raised further concerns about privacy and fairness, especially when used in consumer and retail businesses.

Privacy implications in retail security

FRT is becoming more common in retail settings. It can help with security, reduce theft, and even improve customer service. However, its use raises important legal and ethical questions, especially when it involves collecting and processing personal data.

In the UK, the use of FRT is mainly governed by the [Data Protection Act 2018](#), the [UK General Data Protection Regulation \(UK GDPR\)](#) and the brand-new [Data \(Use and Access\) Act 2025](#). These laws treat facial data as special category data, meaning it must be managed with extra care and specific requirements apply for processing such personal data.

One key issue is transparency. Customers must be clearly told when and why their faces are being scanned. This includes prominent signage at store entrances and clear explanations of how long data will be kept and who it may be shared with. Another concern is data security. Unlike passwords, facial data cannot be changed to mitigate the harmful impact. If facial data is leaked or misused, the consequences can be long-lasting.

Retailers must also avoid using FRT for purposes beyond what was originally stated. For example, if the system is introduced to prevent theft, it cannot later be used for marketing or customer tracking without consent. Any sharing of data with the police must follow strict protocols to avoid turning shops into informal surveillance hubs.

It is crucial that retailers grasp that both their purposes for using FRT and the way the processing of personal data is carried out are both essential elements in ensuring it is lawful. The need for this dual approach is perhaps best illustrated by the intense scrutiny applied by the ICO and the UK Courts to the use of FRT by the UK police in the case of [Bridges v South Wales Police](#).

Here, the Court of Appeal made it clear that even where the purpose for using FRT is justified its application could still be unlawful where data controllers fail to sufficiently address data protection concerns such as transparency, proportionality, and privacy-by-design. Retailers should also expect to have to provide robust evidence of their adherence to such principles when using FRT for security purposes. Indeed, the ICO is currently considering a complaint from a customer alleging that a well-known retailer's use of FRT, wrongly labelled her as a criminal. This matter is still ongoing but has gained wide press coverage. Leaving legal considerations to one side, this matter also highlights the wider and potentially more significant commercial costs associated with having to respond to press criticism and mitigate any potential reputational damage to brands.

Besides data protection problems, one of the characteristic problems with all biometric identification systems, including facial recognition, is the prevalence of false positives and false negatives. This can result in access to services or premises being erroneously denied to the wrong individuals due to misidentification. Furthermore, there is a risk of systematic discrimination against certain groups based on their physical characteristics.

Numerous instances highlight these issues

For example, car awareness systems have shown a tendency to misinterpret the attentiveness of drivers based on their eye shapes, leading to incorrect assessments of sleepiness or distraction. Additionally, there have been reports of biometric systems either unduly complicating or overly simplifying access to face recognition-based devices for people of certain ethnic backgrounds. Such cases underscore the challenges and potential injustices inherent in the deployment of biometric technology and the subsequent backlash from consumers and wider public, affecting the organisation.

European and international perspectives

In the EU, FRT has been considered specifically in the [EU AI Act](#). FRT and other biometric identification systems and their proper usage, especially in real-time systems, were one of the key questions to the end.

Under the EU AI Act, the term **biometric identification** refers to the **automated recognition of individuals** based on physical, physiological, or behavioural traits — such as facial features, voice, gait, or even heart rate. The purpose is to establish a person's identity by comparing their biometric data with entries in a reference database. This process can occur with or without the individual's consent.

Importantly, this definition **excludes biometric verification**, which is used to confirm a person's identity in a one-to-one match — for example, unlocking a phone or accessing a secure area. Verification is generally considered lower risk because it involves the individual's active participation and is limited in scope.

Remote biometric identification, on the other hand, is defined more narrowly and functionally. It refers to systems that identify individuals without their active involvement, typically at a distance, such as through CCTV or live video feeds. These systems are often used to scan multiple people at once, making them capable of mass surveillance.

The EU AI Act further distinguishes between real-time systems, where data capture, comparison, and identification happen instantly or with minimal delay (e.g. live CCTV monitoring) and post systems: where data is analysed after it has been recorded (e.g. reviewing footage after an incident). Remote biometric identification is considered high-risk under the AI Act, and its real-time use in public spaces is largely prohibited, especially for law enforcement, except in extremely limited circumstances.

For retailers operating in the European market, the distinction between these two terms is crucial. A shop using FRT to allow staff to unlock a secure area (biometric verification) is operating under a different legal and ethical framework than one using FRT to scan all customers entering the store (remote biometric identification).

It is also worth highlighting that European regulators, like their UK counterparts, have produced various guidance and rulings on FRT, including warnings by some continental regulators that the use of FRT in supermarkets should be severely limited.

While it seems that the EU approach to this topic is generally stricter than that adopted in the UK, decisions and guidance issued by EU courts and data protection authorities can still be persuasive in the UK.

Furthermore, many large retailers in the UK also have EU operations, which makes it essential for them to understand how they can effectively navigate these cross-border issues.

Clearview AI and Facewatch

In the UK, the contrasting experiences of Clearview AI and Facewatch highlight the importance of legal compliance, transparency, and ethical use when deploying FRT— especially in retail environments.

Clearview AI is a US-based company, which has built one of the world's largest FRT databases by scraping billions of images from public websites and social media platforms without consent of the individuals. These images are converted into biometric profiles and sold to law enforcement and other clients for identification purposes.

As this practice breaches several provisions of the UK GDPR and EU GDPR, [Clearview AI has been banned and fined by data protection authorities](#) in several countries, including the Netherlands, Greece, France, Italy, and Austria. In many cases the company has also been

ordered to delete the data of individuals.

In contrast, Facewatch, a UK-based company, has taken a more cautious approach. It provides a subscription-based FRT service to retailers, helping them identify repeat offenders and reduce shoplifting. Crucially, Facewatch has adopted measures put forward by the UK regulators to ensure its system meets legal standards.

Following a formal investigation, the ICO concluded that:

- Facewatch had a legitimate purpose for using FRT— namely, the prevention and detection of crime.
- The company had made improvements to its system, including:
 - Reducing the amount of personal data collected.
 - Focusing only on individuals involved in serious or repeated offences.
 - Appointing a Data Protection Officer.
 - Implementing safeguards for vulnerable individuals.

However, the ICO made it clear that this approval does not give a green light for widespread or indiscriminate use of facial recognition. Each deployment must be assessed on its own merits, and the balance between privacy rights and crime prevention must always be maintained.

The key difference between Clearview AI and Facewatch lies in consent, transparency, and oversight. Clearview's model — mass data collection without consent — has been widely condemned. Facewatch, by contrast, has shown that FRT can be used lawfully in retail, provided it is targeted, proportionate, and well-implemented.

Checklist for retailers

Retailers thinking about using FRT should follow these steps:

- Avoid systems that rely on broad, unauthorised data scraping.
- Ensure any FRT system is clearly explained to customers.
- Using the technology only for specific, lawful purposes, such as preventing theft.
- Follow good practice to protect individual rights.
- Adhere to privacy-by-design principles, including carrying out controls such as robust Data Protection Impact Assessment (DPIA) to identify and reduce privacy risks.
- Be transparent – clearly inform customers about the use of FRT and why it is being used.
- Get explicit consent where required, especially when dealing with sensitive data.
- Put strong security measures in place to protect the data from misuse or breaches.
- Keep policies up to date to reflect changes in the law or technology.
- Stay up to date with regulatory developments to ensure ongoing compliance.
- Think about fairness and bias – make sure the technology does not unfairly target or exclude certain groups.
- Align your use of FRT with your brand values and mitigate the risk of reputational damage that might be caused by regulatory enforcement action.

Concluding thoughts

This is a complex and fast evolving area of law, where it is important to keep up to date with regulatory developments. [Specialist commercial data advice](#) is essential in managing these regulatory risks and it is also helping retailers understand how they might be mitigated through other mechanisms such as contractual drafting or insurance.

FRT can offer real benefits to retailers, but it must be used responsibly. By following the law and considering the wider impact on individuals, businesses can make sure they use this technology in a way that is both effective and respectful of people's rights.

Contacts

Saara Leino

Professional Development Lawyer

saara.leino@brownejacobson.com

+44 (0)330 045 1289

Francis Katamba

Partner

francis.katamba@brownejacobson.com

+44 (0)330 045 2725

Related expertise

Data protection and privacy

Data protection for retail