Facial recognition technology: the risks unfold

The facial recognition technology (FRT) industry was valued at $3.86 billion in 2020 and is expected to grow at 15.4% per year (*www.grandviewresearch.com/industry-analysis/facial-recognition-market*). Despite the commercial opportunities, businesses that use FRT for either internal or user-facing applications should reassess their data protection compliance. The press is full of stories about naive enthusiasm that resulted in regulatory scrutiny.

While acknowledging the benefits of FRT, the United Nations High Commissioner for Human Rights' report on the right to privacy in the digital age (UN report), which was published on 15 September 2021, highlights the negative, and even catastrophic, effects on human rights of remote biometric recognition, predictive biometrics, people analytics and other artificial intelligence (AI) (*www.ohchr.org/EN/Issues/DigitalAge/Pages/cfi-digital-age.aspx*). The suggested moratoria on the sale and use of high-risk AI technologies, including FRT, in public spaces are, while not quite a deathblow for FRT, a signal that regulation is needed for this fast-growing sector.

While the EU is currently debating a draft Artificial Intelligence Act (AI Act), the UK has consulted on a new data protection regime that would remove unnecessary barriers to responsible data use (*see News briefs "Artificial intelligence: the dawn of a new legal era", www.practicallaw.com/w-031-0858 and "Data protection reform: setting the course for a new direction", www.practicallaw.com/w-032-7584*). For now, FRT compliance remains a moving target (*see box "New laws expected?"*).

Biometric data

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. 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, as highlighted in the Information Commissioner's Office (ICO) report on the use of live FRT in public places (ICO report), which was published on 18 June 2021 (*https://ico.org.uk/media/for-organisations/documents/2619985/ico-opinion-the-use-of-lfr-in-public-places-20210618.pdf*). Organisations often fail to appreciate that the use of biometric data is generally prohibited except in specific circumstances.

Public sector use

FRT is sometimes used in public settings, including schools, transport and public spaces. The UN report places a higher expectation on public organisations in preventing bias and discrimination, and ensuring the explainability of AI-supported decisions, supervision of the system and participation by service users. However, with limited expertise and resources, public organisations may struggle with complex compliance requirements and assertive FRT providers. Due diligence is essential, as FRT providers may end up holding large volumes of government data, which poses a significant data security and function creep risk. The UN report warns that even using identity verification FRT may be disproportionate if no alternative is provided.

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 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 photography 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 judgment being equally unreliable.

The police continue to trial intelligence-led temporary deployment of FRT in public spaces. Data is collected indiscriminately but only images that match targeted individuals will be retained. However, the greater the human rights interference, the more specific the lawful basis of data processing must be. In *R (Bridges) v Chief Constable of South Wales Police*, the Court of Appeal held that the deployment of FRT was unlawful for failing to apply this relativist approach (*[2020] EWCA Civ 1058*). The relevant policy was not specific enough about who could be placed on a watch list and how the police would exercise their discretion. More recently, the Swedish police were fined €250,000 for using Clearview AI, an unlawful application used to match uploaded pictures against a database of billions of facial images scraped from the internet without individuals' knowledge or consent (*https://edpb.europa.eu/news/national-news/2021/swedish-dpa-police-unlawfully-used-facial-recognition-app_en*). A small number of officers used the app unofficially to identify suspects in child abuse and organised crime cases.

Private sector use

Identity-verification FRT systems have become commonplace. However, even this relatively unintrusive application of FRT raises issues of lawful basis under the retained EU law version of the General Data Protection Regulation (*679/2016/EU*) (UK GDPR). It can be difficult to establish legitimate interest coupled with substantial public interest and, while explicit consent may seem easy to implement on devices, it could be invalid if not freely given. Uber's mandatory FRT verification to combat driver substitution resulted in an indirect race discrimination claim against the company when drivers could not be recognised and had their accounts automatically suspended (*www.theguardian.com/technology/2021/oct/05/ex-uber-driver-takes-legal-action-over-racist-face-recognition-software*). To ensure that consent is valid, offering meaningful alternatives to FRT remains an important compliance requirement.

The COVID-19 pandemic has increased the popularity of recruitment software that analyses the body language, facial expressions and voice of candidates to assign them an employability score. However, this kind of processing of data is likely unfair.

According to the ICO report, there remains a high bar for the lawful indiscriminate use of FRT in public places. The Dutch data protection authority (DPA) reprimanded a supermarket for deploying FRT at its entrance to identify

people who had been banned from entering stores (*https://edpb.europa.eu/news/national-news/2021/dutch-dpa-issues-formal-warning-supermarket-its-use-facial-recognition_en*). Unless there was a match, data would be deleted after several seconds. According to the Dutch DPA, the use of FRT outside of the home is banned in nearly all cases, and for good reason. The Dutch DPA said that there is no substantial public interest in deploying FRT for security purposes which will require consent.

In relation to advertising, billboards can be fitted with FRT cameras for audience measurement, monitoring dwell-time at locations or serving targeted adverts at passing individuals. While not unlawful, the ICO concluded that there is no clear justification that the automatic and indiscriminate processing of biometric data in this context is necessary and proportionate without the direct engagement of the individual.

Human rights due diligence

Technology providers often act as data processors and avoid regulatory responsibilities, which fall on unsuspecting customers. Recently, schools in Scotland adopting an FRT-enabled payment system for school lunches trusted that the technology relying on encrypted facial templates did not process personal data. The use of this technology is currently on hold while the ICO investigates. If an FRT provider is confusing data security with data protection, the organisation should choose another provider.

According to the UN report, organisations must conduct human rights due diligence throughout the lifecycle of the FRT system. In the public sector, the updated Surveillance Camera Code expects authorities to avoid manufacturers that are associated with breaches of international law or human rights abuses (*https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1017674/Fraser_Sampson_s_response_to_SC_Code_Revision_FINAL_08.09.2021.pdf*).

Organisations are under pressure to dramatically increase the transparency and explainability of the AI systems that they use. However, if an FRT provider considers its technology a trade secret and has immature policies and procedures, organisations have little hope for oversight reports and auditability of the FRT system. If transparency from the provider is not forthcoming, an organisation's last resort is including the provider's details in its privacy notice and redirecting complaints; however, many providers will be unwilling to deal directly with end users. Organisations should beware of FRT providers using the data to train their algorithms. For example, many providers use standard terms that present "developments" as a service feature but, in essence, this is an opaque permission for the provider to use the data for its own purposes.

Practical considerations

The lawfulness of FRT will hinge on evolving regulatory practice, which must remain aligned with societal acceptance. Practitioners will welcome the UN report's analysis of FRT-related risks but, when considering what is acceptable, experiences from other democracies around the world should not be discounted. The adoption of FRT remains complex, particularly when it comes to indiscriminate automated application, which constitutes FRT's most valuable feature. The government promises to clarify the legal framework in order to encourage the adoption of new technologies. Until then, a measured and conservative approach is advised when deploying FRT.

Organisations should consider whether their legitimate interest basis is well founded or whether it would be better to use explicit consent as a basis for data processing. Transparency, choice, individuals' rights and alternatives to FRT are essential considerations. Looking at what the competition is doing may not be sufficient and a prior consultation with the ICO should be considered. Public sector organisations should be careful not to pursue cost-saving projections that may not materialise if FRT is implemented without proper operational support, as it will likely lead to complaints and investigations.

FRT providers must be held to a high standard and co-operate in the due diligence process. If an FRT provider fails to connect an organisation with the legal team to discuss compliance at a very early stage, the organisation might do well to walk away.

New laws expected?

The UK data protection framework offers flexibility within the boundaries of human rights jurisprudence. No technology is explicitly banned but intrusive data processing would be unlikely to pass the necessity and proportionality tests under UK data protection law. The government's proposed data protection reforms seek to encourage innovation and research by expanding on the permitted processing of special categories of personal data.

Even if the UK takes a path of innovation, it will never be able to compete with the many tech-hubs in countries that do not view privacy as a fundamental right. However, this cannot be the aim of any reform, as any significant reduction in data protection could give rise to human rights complaints and affect the UK's data adequacy status with the EU.

New laws are expected to address the wider risks of facial recognition technology (FRT) and complying with the relativist approach in relation to certain law enforcement use cases. There are calls to permit the police to retain biometric data and allow the further deployment of FRT for law enforcement purposes in order to comply with the state's positive human rights duty to protect its citizens. Unlike the EU's draft Artificial Intelligence Act, the UK does not have FRT-specific product liability laws that remedy privacy infringements. Given the fast pace of innovation in FRT, regulating the providers and manufacturers of FRT systems would seem appropriate.

Alexander Dittel is a partner, and Elizabeth Kilburn is an associate, at Wedlake Bell LLP.