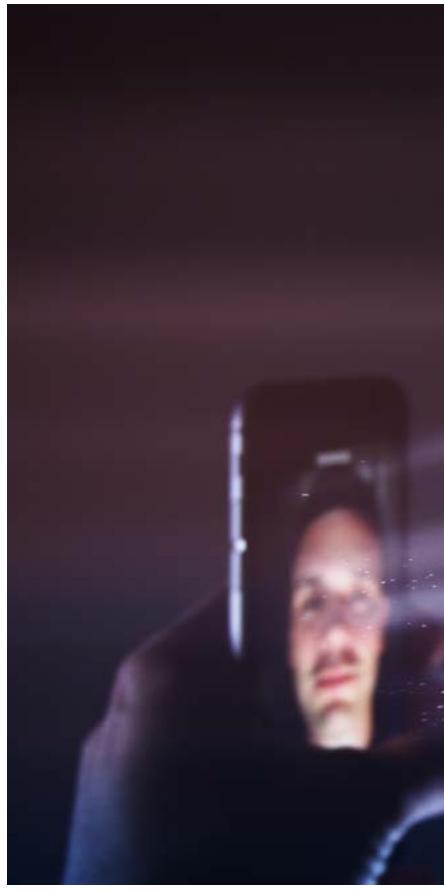


Face value

Facial recognition technologies present both technical and moral issues for the organisations that use them

BY MARTA DUNPHY-MORIEL AND ALEXANDER DITTEL

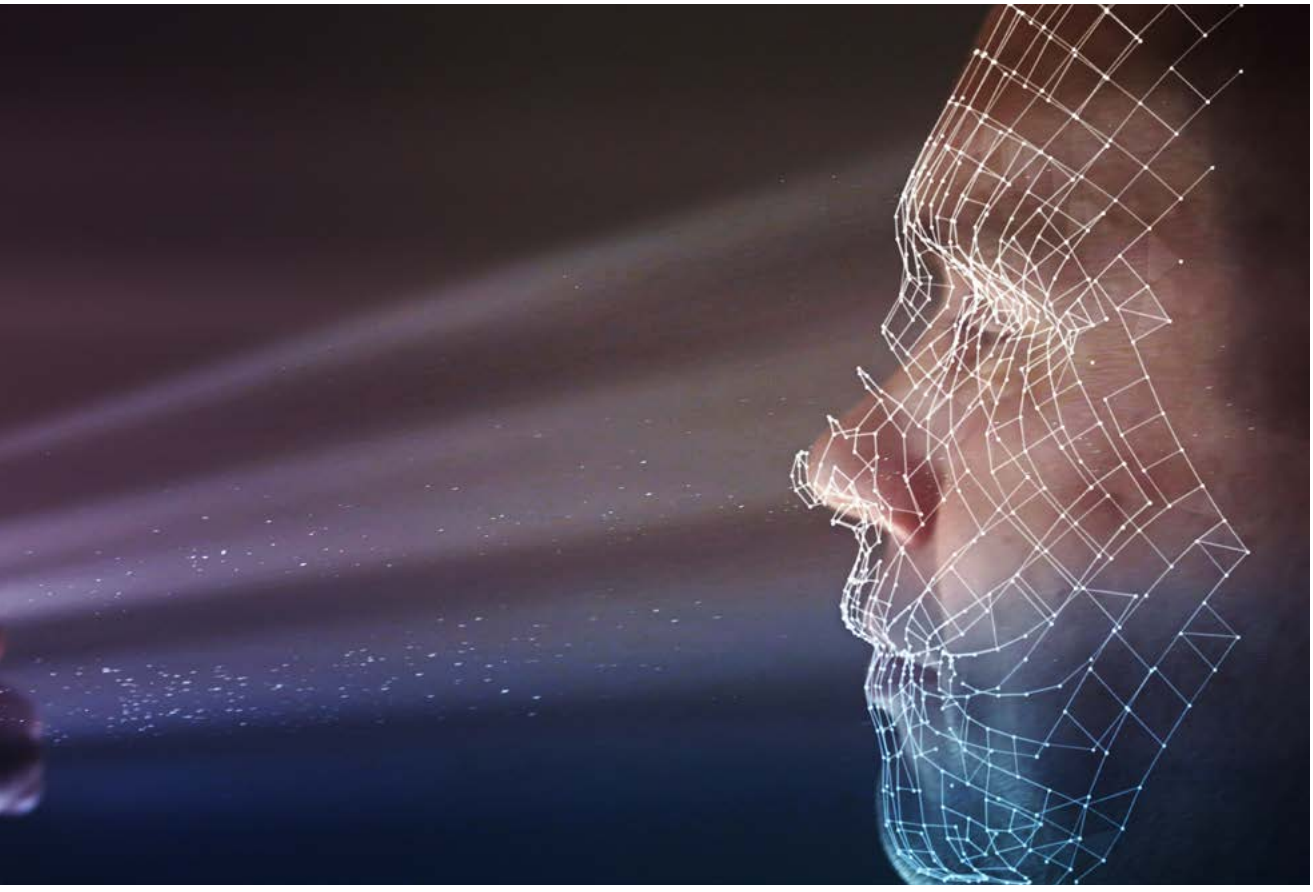
Facial recognition technology (FRT) has found its way into our daily lives, from relatively transparent use of FRT for user authentication on smartphones to the arguably intrusive surveillance when visiting certain countries. Especially in the context of national security, this tool is one of the most polemic pieces of technology created in the last decade. Its defenders argue that it is a useful tool for national security; its detractors explain that it is excessively intrusive and a key tool for an Orwellian state.

In FRT, CCTV cameras record video images of individuals. Those images are analysed by FRT algorithms which scan for distinguishable facial features such as the distances between a person's eyes, the eyes and the tip of the nose, or the width of the mouth, to create a unique biometric data record of an individual. The record is then matched against a database of biometric templates to determine whether the "object" is a person, is male or female, has certain characteristics, is feeling happy or angry or to identify the individual. This processing can be done in real time.

> **The key concerns that the public have around FRT are intrusiveness, bias and lack of transparency**

A useful technology

There is no question that FRT is a useful tool. At an individual level, instead of having to remember all your passwords, you can simply look at your smartphone to access your banking apps. Smartphone apps help you tag people in pictures and organise your photo albums. FRT can also detect when a driver is distracted and alert him or her, or it may slow the car down.



It can also help to cut queues. Airports use facial recognition to speed up immigration checks. One company is proposing to use FRT in cars to keep the passengers safe. Commercial buildings in the UK have tried (and failed) to adopt FRT for access authentication and security surveillance. Amazon has said that even older FRT outperforms human abilities to recognise someone.

Law enforcement agencies across the globe have understood FRT's potential to prevent and detect crime. That has so far included the use of body cams in Los Angeles, police FRT trials in the UK and Germany, and state surveillance in China, which is said to house four billion cameras.

While technology companies rapidly push the adoption of their FRT-related artificial intelligence products, questions about the legality, morality or even ownership of data remain unsolved.

Key concerns

The key concerns that the public have around FRT are intrusiveness, bias and lack of transparency.

While we would hope that we are fairly far away from the kind of ubiquitous surveillance societies depicted in such science fiction films as *Minority report*, there is a concern that recording biometric data may force people to change their behaviour. For example, the deployment of FRT could create a sense of being watched in public that could dissuade people from expressing their views or participating in peaceful protests.

Accuracy issues have cast doubt on the ability of FRT to deliver fair outcomes. This is due to data engineers' failure to adequately train their FRT models on a sufficiently diverse audience. As a result, any automated decision-making which is operated without human intervention will likely not be lawful.

The fear that FRT could potentially be deployed without people's knowledge (concealed, for instance, behind regular CCTV cameras which people have grown accustomed to) has been a common theme as FRT is implemented in different sectors. The

> **There is no question that FRT is a useful tool**

indiscriminate use of FRT will likely result in the unlawful surveillance and profiling of individuals, in breach of their fundamental right to privacy.

Deploying FRT is not impossible, but in order to achieve compliance and user trust, risk managers will have to carry out a thorough technical and legal analysis of the planned implementation (see *Practical steps for risk managers*).

A moral question?

FRT also raises moral issues for organisations. The European data protection supervisor, Wojciech Wiewiórowski, noted that "facial recognition is being promoted as a solution for a problem that does not exist". The convenience and efficiency afforded by FRT do not outweigh our right to privacy. Equally, a balance must be struck between the necessary law enforcement activity and our right to privacy. This is important because satisfying the legal requirement of proportionality will be dictated by the society's attitudes towards privacy.

While we may trust CCTV, we are not ready to trust facial recognition. There is no way to hide from it, and the privacy intrusion is almost absolute. In addition, the system will likely profile individuals relying on a large pool of data which is open to significant abuse.

Scepticism about the use of power is a fundamental part of a democratic society. Universal human rights, watchdogs, judicial review and ombudsmen are supported by the free press, human rights associations, advocacy groups and activists. Without checks and balances, the few would soon control the many.

Is giving up freedom too high a price to pay? According to Wiewiórowski, it is important to look not only at any short-term benefits of allowing the technology but "also the likely direction of travel if it continues to be deployed more and more widely." Striking the right balance in the moment is one thing, but allowing trends that silence our demands for privacy could lead us down a dangerous path.

The same problem does not necessarily arise in China. People there seem to trust the authorities. If you have nothing to hide, you have nothing to fear. The state knows your every move, your family and people you regularly meet, but that is fine. A BBC programme from December 2017 showcased that an arrest can be made within minutes. In an interview, a Chinese police representative said that data is only used if people need help. Otherwise, it is only stored on servers but not used unless needed. FRT also plays a role in the government's social score system. Antisocial behaviour is tracked, and it will affect your score. A low score will restrict your ability to study, travel or run a business. You will be rewarded if you act as is expected of a good citizen. But the unanswered question is who decides what is right or wrong.

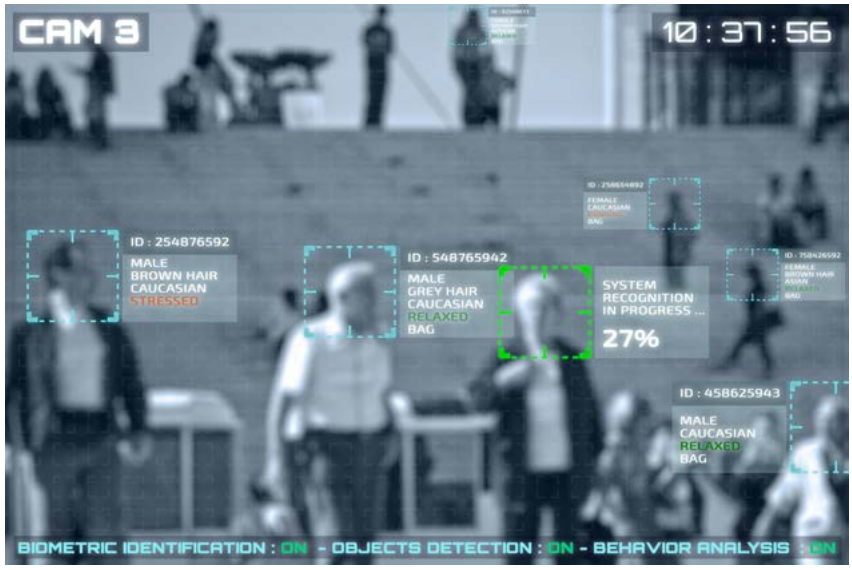
While the Chinese may endorse FRT for security reasons and to discourage behaviour they deem unacceptable, elsewhere attitudes

> **In order to achieve compliance and user trust, risk managers will have to carry out a thorough technical and legal analysis of the planned implementation**

PRACTICAL STEPS FOR RISK MANAGERS

Considerations for the potential implementation of FRT include:

- Establishing a gateway for teams to engage with risk managers. A data protection impact assessment should start soon after the project is conceived.
- Being sure the benefits outweigh the risks. Aside from GDPR fines (up to the higher of €20 million or 4 per cent of worldwide turnover), an even bigger risk is presented by the rise of class action in Europe. Naturally, there will also be reputational risk as technology press indulges in biometric data mishaps. It will help if your teams understand these risks.
- Considering any advance data processing that may be required to train the model or to create an identity database.
- Considering if facial detection may suffice instead of facial recognition. Less intrusive technologies should be preferred if they can achieve a similar result.
- Determining your lawful basis for processing and avoiding relying on alternative bases as this indicates uncertainty.
- Undertaking a mature objective assessment of proportionality, which will be essential to satisfy the human rights requirements. Regulatory guidance should be strictly followed.
- Telling individuals what you are planning. If being honest seems difficult, maybe you need to rethink the project.
- Going over technical details with those who understand them and challenging what data is processed and why.
- If in doubt, prior consultation with the regulator, which may help mitigate the risk, but beware of potential opposition and delays this may cause.



differ. California, for example, has imposed a five-year moratorium on the use of facial recognition in police body cams. Similarly, an early draft of a white paper (*Structure for the white paper on artificial intelligence – a European approach*) suggests that the European Commission is planning a three-to-five year ban on the use of FRT in public spaces. Wiewiórowski questions whether FRT can be ever permitted in a democratic society.

Compliance with GDPR

GDPR compliance in relation to FRT is also an evolving area. The failures in the public and private sector indicate that a high threshold has to be met in order to comply. While a limited police trial of FRT in the UK withstood a judicial review (*Bridges v South Wales Police*), the UK's information commissioner accepted that the matter was decided on its facts but subsequently expressed doubt about the FRT trial. The judiciary remains focused on this developing area of law. The new Media and Communications List in the UK's High Court will further contribute to the judiciary's expertise, which is already highly regarded around the world.

Compliance becomes more difficult when the use of FRT triggers GDPR provisions relating to biometric data. This will not be the case if the technology is merely used for facial detection, i.e. not seeking to uniquely identify an individual but rather segmenting the audience into categories according to age, gender, facial attributes, mood and so on. GDPR will still apply, but it will be easier to satisfy the data protection principles. This is probably why Amazon's Rekognition FRT refers to "predictions" rather than "matches", and results are provided with a similarity score rather than uniquely identifying a person. Even 99 per cent similarity does not guarantee a positive match, Amazon claims.

However, when we talk about FRT in its true sense – where it is linked to a reference database to identify or "single out" individuals – GDPR provisions relating to special categories of personal data come into play. Any indiscriminate monitoring of individuals in public spaces will unlikely meet the compliance threshold.

Recent cases have highlighted these difficulties. A Swedish school in the Skellefteå municipality using FRT for an attendance trial was fined over £16,000. The school's reliance on parental consent failed due to the relationship of dependence, which rendered the consent invalid. Similarly, employers will not be able to rely on consent of their staff. The school's alternative legal basis, which was a legal obligation to carry out effective case handling, also failed because, as drafted, the obligation was not deemed to cover the use of intrusive automated technologies. The use of FRT in the trial was disproportionate, and so was a proposed FRT trial aimed at ensuring that students pay attention in class at schools in Nice and Marseille in France.

When it comes to the use of FRT by law enforcement, the UK Data Protection Act 2018 imposes a "strict necessity" test. Challenged by Liberty, a human rights advocacy group, South Wales Police was successful in defending its activity in court. However, the information commissioner subsequently rejected that a fair balance between the "strict necessity" of the processing and the rights of individuals had been struck. It is likely that as a minimum, any future surveillance will have to be targeted, intelligence led (based on specific cause or reasonable suspicion) and time limited. A detailed written analysis and judgment on proportionality will be required, justifying why less intrusive means to achieve the desired objective had been discounted.

We expect to see new legislation in future banning certain deployment of FRT under threat of criminal sanctions, while at the same time providing a lawful basis for certain convenience and efficiency-enabling use of FRT, such as employee authentication. Any such law will no doubt come with strict requirements of transparency, accountability and governance.

Marta Dunphy-Moriel is partner and interim head of data protection and privacy, and Alexander Dittel is commercial technology senior associate at the law firm Kemp Little.

> **Any indiscriminate monitoring of individuals in public spaces will unlikely meet GDPR's compliance threshold**