Facial recognition technology: Supporting a sustainable lockdown exit strategy?

May 2020

DLA Piper - Multiple Authors* [1]

Technology has played a dominant role during the lockdown and will be a key aspect of ensuring the transition back to normality is successful. This article discusses recent trends, particularly in Ireland, Denmark and China, regarding the adoption of facial recognition technology (FRT) as a result of the COVID-19 pandemic. We look in more detail at some of the pre-pandemic use cases for, and concerns about, FRT, and consider the key aspects of data protection law when adopting such technology solutions.

Exit through technology

Age, geographic, sector and other forms of segmentation and social distancing will become the longer-term norm as countries transition out of lockdown. Use of key measures such as technology-enabled contact tracing are playing an important part, particularly in jurisdictions at a more advanced stage of transition from lockdown. It has been suggested that a 60% rate of adoption of tracing app usage could end the epidemic. This requires the population to suspend concerns about privacy for a greater common good; to trust that the benefits outweigh the risks and that the technology is designed and used in a way that strikes the appropriate balance.

During lockdown and as we move out of lockdown, certain essential services and sectors such as medical device and food manufacturing, telecoms and core banking services have remained operational or will gradually expand before others.

In Ireland, a large food producer has put an FRT solution in live use as part of staff protection measures, to avoid staff needing to sign in manually at the start and completion of their shifts. There are already signs of a move to germless and contactless security and access control systems. One Chinese company has confirmed its masked facial recognition program is at a 95% accuracy rate and noted a surge in requests for technology at entrances to premises. At the moment, these are predominantly from hospitals at the centre of the outbreak in China wanting to ensure that nurses wearing masks, who needed access confirmed at a distance, are admitted to work. And the technology is advancing: facial recognition technology can be connected to a temperature sensor, measuring subject's body temperature while also identifying their face and name.

Companies looking to adopt such technology need to consider the restrictions and balances set out in the existing legal framework, taking into account, in particular, that what is necessary in a lockdown scenario may not be necessary when relative normality returns. An interesting position taken by some of the Asia privacy regulators is that, according to the Universal Declaration of Human Rights, the right to life is an absolute right, whereas the right to privacy is a qualified right. They are, therefore, looking at privacy considerations in connection with the pandemic through that lens. In this article, we take a closer look at some of the more established use cases for facial recognition technology and how those

[1] * **Mark Rasdale, John Magee, Cezary Bicki & Eilis McDonald (DLA Piper, Ireland), Marlene Winther Plas & Emil Agerskov Thuesen (DLA Piper, Denmark), (Carolyn Bigg, DLA Piper, Hong Kong)**

checks and balances apply to them.

What is facial recognition technology?

Facial recognition was first researched in the mid-1960s by Woodrow Blesdoe and Helen Chan, who used computer programming to match a large database of mugshots with a photograph. Their method involved manual extracting of features from photographs and later inputting them into a computer system that compared the pictures. Funded by an unnamed intelligence agency, the project was never widely published and was limited by technological constraints. Fast-forward 50 years, and FRT offers great opportunity, effective solutions and some high-profile challenges.

Mass surveillance concerns, perceived invasion of privacy, inherent bias risk and general lack of understanding of the use cases for the technology are among the main social and political concerns in relation to FRT. Much of the concerns relate to trust. In May 2019, San Francisco became the first US city to ban the use of FRT by any local agencies, including law enforcement. Other cities followed suit in July, and in October 2019 California introduced a state-wide ban on using FRT on police body-worn cameras.

Californians cited, as their most common concerns, mass surveillance, invasion of privacy and inherent systematic bias that may disadvantage minority groups. Various communities in California, including LGBTQ and Muslim, have reportedly been subject to local government profiling, so there is an underlying lack of trust of what is seen as law enforcement agencies adding yet another tool to their surveillance arsenal. In March 2020, the Washington state legislature passed a public sector facial recognition privacy bill that imposes extensive restrictions and conditions on government use of FRT, the effect of which is likely to slow deployment of the technology in the state.

And yet, the benefits of the technology continue to drive an increase in the rate adoption of FRT solutions internationally.

In turn, legislators and regulators are increasingly being required to consider application of existing laws, in particular data protection law, to use of FRT.

Use of facial recognition technology can, but won't always, involve the collection of biometric data. It must allow for the unique identification of an individual. Under Article 4(14) of the General Data Protection Regulation (GDPR), biometric data is defined as:

"Personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic (fingerprint) data".

FRT offers a range of use cases, but can be broadly categorised as:

- **Verification FRT**: holds one piece of biometric information against which it compares various samples that are presented.

Smartphones

The most widespread use case of verification FRT is to be found in smartphone functionality allowing access through verification of facial features. After the first scanning, the phone holds the biometric data of the user's face and checks whether what is presented to it while trying to unlock the phone matches the data it holds.

- **Identification FRT**: checks samples against all biometric references in its systems and identifies an unknown person. More advanced forms of Identification FRT include real-time scanning and analysis known as live or automated facial recognition, the lawfulness of which has been questioned by academics in the Met Police trial (discussed below) and before the courts in the South Wales case, but which may be more widely accepted in other parts of the world, such as Asia. Consent, legal basis and transparency were some issues that emerged in the course of judicial and academic scrutiny regarding the commercial application of Identification FRT.

It is noticeable that in parts of the world where explicit consent is relied on to legitimise data collection, including biometric data collection, Identification FRT is more widely accepted and commonplace (with compliant safeguards in place).

South Wales Police: Technology use case

The mechanics of the Identification FRT as described in the case:

- **Creating a watchlist:** A database of images against which the live facial recognition (LFR) images were going to be compared would be compiled from the police database created in the course of the normal policing activities (mainly custody photographs). The facial features extracted from the images were then turned into numerical values. The watchlist included persons wanted on warrants, individuals who had escaped custody, persons suspected of committing crimes, and missing persons. Including a person on a watchlist was not based on a suspicion that the individual might be present in the area of deployment.
- **Acquiring a facial image:** CCTV would capture a moving image when the person was in the camera's field of view.
- **Face detection:** the software would detect human faces and isolate the individual.
- **Feature extraction:** the software extracted the unique facial features from the image of each face.
- **Face comparison:** extracted facial features were compared to those held on the watchlist.
- **Matching:** while matching, the software would create a "similarity score" – a numerical value indicating the likelihood that the images match. The threshold could be set at a desired level to indicate when the match is found. Matches were then reviewed by a police officer to ensure accuracy. If no match was made, there was no further action. Where there was a match, intervention officers were engaged and only intervened if satisfied that the match was in fact

a suspect.

Not all FRT use-cases are so intrusive, for example, FRT that can detect the presence of a face but does not determine who the face belongs to. An example of this is the technology in a smartphone able to detect how many people are in a photo by showing a square around their faces. Indeed, in some parts of the world (such as Hong Kong and in public spaces in Singapore), this form of data collection might not even constitute personal data collection if the intention is not to identify data subjects.

The benefits of the technology are clear from some of the early adopters. Car manufacturers, such as Ford, are working with tech companies to install facial recognition in their vehicles. The FRT will learn to recognise the primary driver and other regular drivers such as family members, and the car settings will adjust depending on who is sitting in the driving seat. Banking apps use FRT as a way to increase security when logging in or to authorise payments. Facebook has been using FRT since 2014 when it launched its DeepFace program. Its FRT is able to suggest tagging a Facebook user based on them being previously tagged in other photos.

As noted above, the uptake of FRT has been particularly high in China and other parts of Asia where consumers can – and routinely do – scan their faces to pay for groceries or withdraw money, which – provided explicit consent has been obtained, and other safeguards are in place such as avoiding excessive processing, restrictions on sharing, data security – is seen as a convenience and a preferred personalised service rather than a practice raising concerns. This has in turn led to wide acceptance of FRT during the lockdown as part of prevention and control measures against the virus, and we expect it will continue to be a widely accepted measure as China and other parts of Asia get back to business as the lockdown ends.

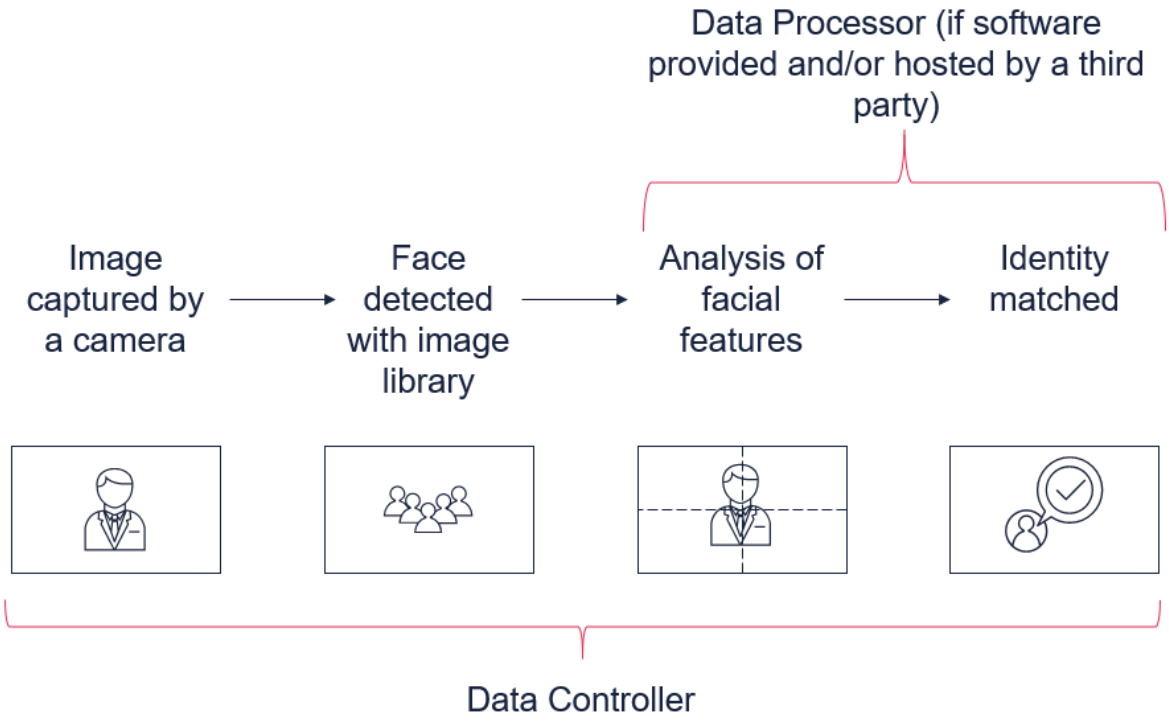
The primary issues to consider are the extent to which the law and regulation ought to be adapted to address the sometimes valid concerns regarding trust, and the point at which the regulation dilutes the social benefits of FRT innovation.

Current EU legal framework

GDPR: Key principles

In Europe, the data protection law relevant to FRT is found mainly in GDPR.[2]The diagram below identifies the typical data controllers/processor dynamic when a FRT solution is being used.

[2] The Law Enforcement Directive, as enacted in EU jurisdictions, will apply where the FRT is used by criminal law enforcement bodies. The key provisions under GDPR are Article 4 which provide definitions of "personal data" and "processing," Article 6 dealing with the lawfulness of processing, Article 7 dealing with consent, Article 9 addressing special categories of data, and Article 22 on automated individual decision-making.



Under Article 9(1) GDPR, biometric data constitutes "special category data," processing of which is generally prohibited unless one of several specific exceptions applies.

Not all data collected using FRT will be classified as special category data: Article 9(1) GDPR specifies that biometric data will be considered a special category data only when it is used to uniquely identify someone. If, for example, FRT is used to detect whether a customer is male or a female, it will not necessarily uniquely identify an individual and could therefore fall outside the scope of special category data. Another instance would be when digital photographs of individuals are processed and the image data is not further used (for example, to create a digital profile).[3] Importantly, Article 9 is one of the GDPR provisions that left a fair degree of latitude to Member States to legislate further at local level. Accordingly, this aspect of GDPR is less harmonised across Europe and presents a further challenge to businesses seeking to roll out FRT solutions designed to capture special category data on a pan-European basis.

While processing personal data, the core principles of data protection from Article 5 must be adhered to. Some of the principles key to FRT include:

Purpose limitation

The data must be collected for a specified, explicit and legitimate purpose that is defined at the time the personal data is collected.

[3] UK Information Commissioner's Office Guide to Data Protection and Special Category of Data

Transparency

Ensuring clarity of purpose enables compliance with the transparency principle, which further obliges the data controller to provide data subjects with information regarding the processing of their data in a clear, concise and comprehensible format, in the form of a fair-processing notice. Delivery of adequate notices can pose a significant challenge regarding FRT use. For example, individuals may already be in the vicinity of an FRT-enabled camera by the time they're aware of signage.

Data minimisation

The data minimisation principle requires data controllers to collect the minimum amount of data required for the defined purposes. Further, the processing must be balanced against the rights of the data subject.[4]

Data security

Appropriate technical and organisation security measures should be in place to ensure the security of data obtained from FRT solutions. Defining what is appropriate requires an assessment of various measures including the nature, scope, context, and purposes of the processing, and the risk of varying likelihood and severity for the rights and freedoms of natural persons. In most FRT solutions, meeting this standard will require a significant investment in security

No automated decision-making

Article 22 gives data subjects the right not to be subject to decisions based solely on automated processing – i.e. without human intervention. It is, however, permitted with express consent, if expressly authorised by law, or for reasons of substantial public interest.

When processing special category of data, an Article 9 exemption must be satisfied in addition to one of the lawful bases from Article 6. The main bases for processing biometric data include those of public interest, legitimate interest, and consent, each of which comes with limitations and challenges.

It is therefore necessary to understand in detail the functionality of the technology and the scope of the proposed use case before drawing any conclusion as to its legality. A good illustration of this is in the South Wales Police case.

***In R (Bridges) v Chief Constable of the South Wales Police*[5]**

The lawful use of live facial recognition (LFR) has been tested in the UK, reaching the High Court in September 2019, when a civil liberties campaigner brought a case against South Wales Police's use of LFR in 2017 and 2018. The court held that it was lawful for the South Wales Police to use LFR, though the case is being taken to the Court of Appeal.

The claimant challenged the general lawfulness of the LFR use and the adequacy of the legal framework relating to LFR. The LFR use was challenged on three grounds:

- **Human rights:** it was claimed that the use of LFR interfered with Article 8.(1) of the European Convention on Human Rights.

[4] Irish Data Protection Commission, Quick Guide to the Principles of Data Protection
[5] [2019] EWHC 2341 (Admin)

- **Public law:** it was claimed that South Wales Police failed to comply with its public sector duty under the UK Equality Act 2010, s. 149(1).
- **Data protection:** The main point of contention related to what constituted personal data. South Wales Police argued that the only personal data it was processing pertained to those people on the watchlist. The court applied a concept of *individuation*, defined by the UK Data Protection Act 1998, which stated that personal data is data of a person who can be identified by one or more factors specific to their physical, physiological, mental, economic, cultural or social identity.

The court found that the data from the LFR did constitute personal data, as it distinguished a person out from others. The biometric facial data was qualitatively different and comprised personal data as it permitted immediate identification of a person. South Wales Police was therefore required to adhere to the data protection principles. The court found that the LFR involved the sensitive processing of the biometric data of people captured by CCTV cameras and ruled that it was necessary for law-enforcement purposes. Key to South Wales Police's case was the fact that they had applied the general data protection principles to their use of LFR: they carried out and were able to demonstrate valid Data Protection Impact Assessments and created and actively used a policy on sensitive processing for law-enforcement purposes. Equally, they demonstrated that they had balanced the processing against the rights and freedoms of data subjects by showing that the processing was limited to specific areas where severe crime and disruption had been evident in previous years. In the surveillance sphere, it seems that if commercial users of LFR are able to demonstrate strict adherence to general principles of data protection, human rights and public law, then the use of LFR for specified purposes may become more mainstream.

Legal basis

Substantial public interest

This ground is most relevant to public bodies and organisations carrying out tasks in the public interest. In order to rely on it, the data controller must show that it is exercising official authority and discretionary powers. Additionally, the task or the function of the data controller must be laid down by the EU Member State's law. While that does not require explicit statutory provision, the data controller's tasks, functions or powers must be sufficiently clear and precise. This ground is therefore of limited use to private organisations. According to the Irish Data Protection Commission (DPC), for example, public authorities and legal persons governed by public law are the organisations most likely able to successfully rely on this ground. This would include the police using FRT as part of crime prevention, or a public authority introducing FRT authentication to access their services.

Of the European data protection authorities, the DPC is notable for its focus on enforcement efforts around public authority and police use of new technologies. Over half of the domestic statutory inquiries opened by it since the introduction of GDPR in Ireland are investigating local authority and law-enforcement use of technologies including CCTV, body-worn cameras, automatic number plate recognition-enabled systems, drones and other technologies.[6]

The application of this legal ground is not so limited in every jurisdiction, as illustrated recently in Denmark in the *Brøndby* case:

The *Brøndby* case

Live facial recognition FRT was successfully implemented in Denmark in 2019 by one of the largest Danish football clubs, Brøndby IF. To address the problem of stadium hooliganism, the club decided to implement LFR in order to identify the blacklisted individuals attempting to enter its stadium.

In adopting the LFR, Brøndby liaised with the Danish Data Protection Agency (DDPA), which approved the processing as necessary for reasons of public interest, as required for private organisations under the Danish Data Protection Act.

Prior to liaising with the DDPA, Brøndby also carried out a data protection impact assessment, considering the rights and freedoms of natural persons.

While approving the use of LFR, the DDPA considered that:

- neither the video footage from the stadium, nor the images were retained on the system; and
- the decision-making process was not automated (similar to the South Wales Police case).

The system would flag the match, sending an alert to a trained security professional, who made the final decision on whether there had been an accurate match.

A formal Data Protection Impact Assessment (DPIA) is mandatory under Article 35 GDPR in circumstances where data processing "is likely to result in a high risk to the rights and freedoms of natural persons," particularly when a new data processing technology is being introduced. Guidance issued by the European Data Protection Board (EDPB) specifically references "innovative use or applying new technological or organisational solutions, like combining use of finger print and face

[6] Data Protection Commission Annual Report 2019

recognition for improved physical access control."[7] If a high risk to the data subject is found by the DPIA that cannot be mitigated by the controller, the relevant organisation's competent data protection supervisory authority must be consulted for both GDPR and Law Enforcement Directive purposes.

Legitimate interests

This ground offers a degree of flexibility for private companies wishing to use FRT, and cannot be relied on by public bodies. This ground may be relied on only if the data collected is not categorised as special category data.

Reliance is conditional on balancing the identified legitimate interests with the interests of the data subject(s). The legitimate interests covered by this ground include those of the controller or the third parties. The scope is reasonably broad, and the DPC cites commercial, individual interests and societal benefits as applicable.[8] It further suggests that a legitimate interest is likely to exist where there is a "relevant and appropriate relationship" between the data subject and the controller, for example between a service provider and a client. It is worth noting, however, that while relying on this ground, a careful assessment of the legitimate interest against the data subject's interest, rights and freedoms should be undertaken. Such balancing exercise should also consider whether a data subject can "reasonably expect" that the processing of their personal data might occur for the purposes of the legitimate interest. A retailer using FRT to speed up payment processing might, for example, fall into this category.

EDPB Guidelines provide further clarity on the use of FRT. In relation to surveillance use in particular, the EDPB advises that when seeking to rely on legitimate interests due to a "real and hazardous" situation (for example, theft), it will not be enough to simply produce statistics demonstrating high levels of crime in the designated area. The legitimate interest must be of "real existence and has to be a present issue."[9]

Necessity

In the case of both public interest and legitimate interests grounds, it must be shown that the processing is necessary to carry out the tasks or achieve a purpose. The processing also must be reasonable and proportionate. Thus, if the controller can achieve its aims in a less intrusive way, the above grounds will not be satisfied.

GDPR fine in Sweden

The lawful application of FRT has also been recently considered in Sweden, where a high school introduced FRT trials in order to monitor its students' attendance in class. However, it was subsequently fined circa EUR20,000 for a GDPR breach. The Swedish Data Protection Authority challenged the use of FRT, as students' attendance could have been verified by less intrusive methods, and decided that students' consent was not freely given, as they were in a position of dependence with the school board.

[7] EDPB Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679(WP 248)

[8] Data Protection Commission, Guidance Note: Legal Bases for Processing Personal Data, December 2019

[9] EDPB European Data Protection Board Guidelines 3/2019 on processing of personal data through video devices (version for public consultation), adopted on 10 July 2019

Necessity of processing under Article 5 GDPR is a key consideration for determining whether the use of FRT is lawful. This applies to both verification and identification FRT: the EDPB advises that the use of surveillance should be considered only if it is suitable and adequate to achieve the desired purposes. If other less intrusive options are available to achieve safety, these should be exhausted first. In relation to identification FRT, for example when accessing a building, there should always be an alternative option to verify someone's identity, for example with a security pass or signature.

Consent

Given the limitation of the legitimate interests and public interest grounds under GDPR, reliance on consent, while still difficult, is more likely to be the correct legal basis for many private sector companies using FRT. Relying on consent is difficult due to practical obstacles in obtaining it and the conditions that need to be satisfied for it to be valid. This is, of course, in distinct contrast to other parts of the world such as Asia, where express or explicit consent is the key requirement to legitimise (general, sensitive and biometric) data collection, use and disclosure under the various local data protection frameworks; and where, unlike in the EU, there are no challenges to proving consent was given. [10]

As defined in GDPR, a consent must be expressed by a statement or a "clear affirmative action" that has to be unambiguous. Consent cannot be therefore inferred by silence, inactivity or pre-ticked boxes. The consent should be specific and informed; the data subject needs to understand what exactly they are consenting to. Most importantly, the consent needs to be "freely given." A practical example of consent can be found in many smartphones, which give access to some of the their features through FRT. The consent is given freely, can be withdrawn by deleting the face scan, and the features can be accessed by alternative means, like a passcode.

However, consent will not always be a viable legal basis. Where FRT involves the collection of biometric data to identify individuals, reliance on consent as a lawful basis for processing will be possible only where the consent is explicit. In practice, providers and suppliers of FRT are far more likely to obtain consent to use verification FRT, rather than identification FRT, which in current use cases is more often associated with surveillance. Documenting consent is easier in the case of verification FRT, since an individual usually has to agree to using it (for example, setting up face scan to unlock your smartphone).

The very nature of identification FRT makes obtaining consent more challenging when using identification FRT in a certain area. How would consent of individuals be obtained? As argued in the Met Police study, displaying messages that FRT is used is unlikely to be enough to satisfy the threshold of explicit consent, not least because data subjects are likely to already be in the vicinity of the FRT-enabled cameras by the time they are aware of it. Another practical obstacle comes from the fact that the data subject has to be able to withdraw consent at any time.

Group consent poses a challenge too. As demonstrated by Facebook's use of FRT in their photo-tagging tool, while one data subject may explicitly consent to the use of FRT to identify them in images, others who are affected by the technology may not have. The FRT would be required to compare the consenting data subjects face against many images of potentially non-consenting individuals to make

[10] Taking Singapore by way of example, under the "Consent Obligation" in sections 13 and 14 of the Personal Data Protection Act 2012 and accompanying advisory guidelines (including Chapter 12 of the "Advisory Guidelines on Key Concepts in the Personal Data Protection Act and Chapter 4 (Photography, Video and Audio Recordings) of the Advisory Guidelines on the Personal Data Protection Act for Select Topics)

an accurate tag.

UK Metropolitan Police FRT trial

In the UK, LFR has been trialled by the Metropolitan Police for three years, up to July 2019. The technology involved a camera system set up for the purpose of the trial in specific points at London's busy intersections and streaming images in real-time to the facial recognition system. The software would then process the image in order to identify a face and compare it against a watchlist to search for matches. In case of a match, the police were alerted to take action. Any match was stored for 30 days, and the images that did not produce a match were immediately deleted. The system did not create any databases. The issues that arose relate to consent and discrimination bias.

In accordance with the Surveillance Camera Code of Practice[11] (a guidance document to police authorities), which the Met relied on, "consent to surveillance must be informed and not assumed by a system operator."[12] In the course of the trials, consent was claimed to be obtained by displaying signs informing the public of the trials. The method of obtaining the consent was challenged as the placement of the signs left the public with little choice as in most cases, an individual entered the cameras' field of view within seconds of encountering the sign. In some cases the signs were only visible when the individual entered a field of view. The meaningful aspect of consent was the ability of the individual to make an alternative choice. The options available to the public during the trial varied from crossing the road to making an 18-minute detour. The degree to which the consent is informed and meaningful may, therefore, depend on the implementation methodology.

In considering the implementation of FRT, identification of the correct legal basis is critical but can be complex and, where the technology is being used on an international basis, careful consideration of the significant regulatory, compliance (and cultural) differences across jurisdictions is essential. A detailed compliance and risk analysis should be done prior to going live with the technology and, in the EU at least, this analysis should be underpinned by a data protection impact assessment.

In most cases, introduction of an FRT application will require a DPIA to be conducted. In Ireland for example, the DPC guidance recommends that a successful DPIA involves:

- identifying whether a DPIA is required;
- defining the characteristics of the project so that an assessment of the risks can take place;
- identifying data protection and related risks;
- identifying data protection solutions to reduce or eliminate the risks;
- signing off on the outcomes of the DPIA; and
- integrating data protection solutions into the project.

[11] The closest equivalent in Ireland is DPC's Guidance For Data Controllers on the Use of CCTV
[12] Surveillance Camera Code of Practice," June 2013, paragraph 1.5

FRT solutions can deliver positive outcomes – and indeed may prove a very useful tool as part of a range of measures that help businesses restart following the COVID-19 outbreak and lockdown. But the privacy implications are significant, and so businesses must take a thoughtful, measured and robust approach when considering those implications and balancing the risks.

There is no substitute for an appropriate risk mitigation and compliance with this approach, even in a lockdown. The risk and impact assessment will apply at a point in time. The balance of interests in a period of lockdown due to a public health crisis may be quite different when relative normality returns.