9-2020

Reflections on the use of facial recognition technology during COVID-19

Gary Kok Yew CHAN
Singapore Management University, garychan@smu.edu.sg

18. Reflections on the use of facial recognition technology during COVID-19

Gary Chan[526]

During the COVID-19 pandemic, infected persons have been quarantined in segregated facilities. Individuals who have been in contact with infected persons may be subject to self-isolation measures or stay-home notices. Technological tools such as proximity and contact tracing apps are used to identify those who have been in close contact with infected persons. The contract tracing QR code used in Singapore's SafeEntry requires the submission of personal information (including names and identification numbers) prior to entry into certain public places such as malls, factories and restaurants. Robots, in addition to designated human officers, have been deployed to maintain social distancing in public places.

Beyond these measures and technologies, facial recognition technology (FRT) is being used for public health surveillance during the COVID-19 pandemic. At the workplace, FRT has been utilised to detect employees with thermal fever and to ensure they wear masks. CCTV cameras with FRT installed monitor those that are subject to quarantine and self-isolation measures in Russia. In China, FRT scans individuals in crowds for signs of thermal fever and identify persons even with masks covering their faces. The UK government is exploring giving out digital certificates or "health passports" through the use of FRT and coronavirus testing to certify that the individual is entitled to return to the workplace. Singapore uses an automated gantry system for temperature screening in hospitals to facilitate contact tracing via facial recognition software.

The use of FRT is by no means widespread or uniform across the globe. There are, understandably, serious concerns with privacy and bias. San Francisco was the first US city, followed by Somerville and Oakland, to ban facial recognition software. Washington has placed significant controls on public sector use of FRT. The European Commission had originally intended to impose a five-year moratorium on facial recognition but subsequently allowed individual EU states to make their own decisions. The deployment of live facial recognition software (Automated Facial Recognition (AFR) Locate) by the South Wales Police (SWP) on public streets was challenged by Mr Edward Bridges, a civil liberties campaigner, in the UK courts on privacy grounds. In addition, concerns over FRT have also been voiced in China about the possible leakage of personal information and tracking of their movements.

[526] Professor of Law, Singapore Management University. This research is supported by the National Research Foundation, Singapore under its Emerging Areas Research Projects (EARP) Funding Initiative. Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not reflect the views of the National Research Foundation, Singapore. I am also grateful to Ian Chiang, SMU law graduate, for his research assistance.

Even before the COVID-19 pandemic, FRT had already been used in criminal law enforcement, border controls, and to facilitate the search for missing persons. Can FRT use not be extended to public health surveillance in a pandemic of COVID-19 proportions? As it stands, the global fatality count has exceeded 630,000 and infections have soared beyond 15 million. How serious are the issues of privacy and bias? How do they weigh against public health concerns? Can they be mitigated in any way?

Privacy, Bias and Public Health

FRT uses statistical techniques to detect and extract patterns from data and match them with patterns stored in a database. The FRT process starts with the face image (probe) which is "normalised" based on certain standard facial features. The features are extracted to create a biometric template which is then used to compare with images stored in a database (or watchlist).

To begin with, FRT is more controversial than proximity and contact tracing apps that are downloaded by users on a voluntary basis. In Singapore's TraceTogether mobile app, for example, the user of the app would be required to provide information of the contacts recorded on the phone to the government only if he is infected by the coronavirus. Unlike proximity and contact tracing apps, FRT may be used covertly without the explicit consent of the people in public streets. It is also susceptible to "function creep" (that is, the gradual extension of FRT use into expanded databases and purposes).

Facial images constitute a unique biometric identifier of the individual. Intrusions into personal privacy adversely affect human dignity and can even result in tangible losses (e.g. of employment prospects). One can suffer from infringements of privacy even in a public place, based on the "reasonable expectation" test. FRT does not only have the capacity to intrude into individual privacy rights but may indirectly generate a "chilling effect" on freedom of movement, assembly and association as well as freedom of speech.

But privacy interests or rights are not absolute. In the face-off between privacy and public health, a measure of personal privacy at the very least should arguably be sacrificed for the sake of preserving the individual's life and the lives of the fellow members of his community who are seriously threatened by the pandemic. In fact, apart from human lives, the pandemic has threatened the economic viability of businesses, livelihoods of workers and social cohesion in certain countries due to the consequent lockdowns. Public health may be used to justify limiting the exercise of other fundamental rights such as privacy provided the limitations represent the least restrictive alternative (UN Committee on Economic, Social and Cultural Rights, General Comment No. 14 on "The Right to the Highest Attainable Standard of Health"). Furthermore, information

obtained from FRT and other surveillance methods can contribute to a better understanding of how the virus is spread within the community.

Bias can arise due to the nature of FRT itself and the database of stored facial images. Depending on the exact FRT used, bias against certain minority groups may be attributed to features built into the technology. With a standard template created from a set of facial images, deviations from the standard template (e.g. the images of minority groups in a population) would be recognised by the FRT more easily. Studies have referred to the variations in the performance of different FRTs with respect to age, gender and ethnicity.

Discrimination is essentially about the differential treatment of person in similar circumstances based on certain protected characteristic or attributes. Unlike privacy rights, equality guarantees and non-discrimination provisions are not normally subject to overriding considerations such as public health or national security though they may stipulate the scope of application (e.g. the prohibited grounds of discrimination).

The major concerns in the US are the use of FRT to intimidate and oppress certain minority communities and marginalised groups and its tendency to endanger civil rights and liberties. A National Institute of Science and Technology study indicated that the likelihood of false positives for Asian and black faces was significantly higher than for white faces. IBM has decided not to offer facial recognition software for surveillance and racial profiling in the midst of protests in the US over the death of George Floyd.

Despite these concerns, the fact is that FRT offers significant benefits in its sheer scale and speed of detecting facial images via machine learning algorithms as compared to human capacities. It offers immense potential in law enforcement work in preventing and reducing the incidence of crimes and public health surveillance. Furthermore, public attitudes against FRT use are by no means singular or monolithic; apparently, attitudes to FRT vary depending on the type of use. Based on a poll, the people in the UK, for example, seemed to be more comfortable with FRT use for policing and border control purposes as compared to its use in daily life such as in public transport, schools, supermarkets, and at the workplace. Thus, justifications for FRT use may be made by reference to the potential benefits, the level of public trust, the need to limit the scope of use, and taking into account the risks to privacy and bias.

Safeguards

Even if FRT were to be justified for public health surveillance, safeguards must be put in place. One safeguard pertains to the need for transparency regarding how the images in the watchlist are

selected. If FRT were to be allowed for COVID-19 surveillance, one legitimate question is who should be on the watchlist. As a starting point, it should as far as possible be limited to people who pose serious danger to the community (e.g. those under quarantine orders for the period of the quarantine orders and those who have flouted and are likely to disregard quarantine orders). Whether it should extend to those imposed with self-isolation or stay-home notices and beyond is more debatable.

The English High Court in *R (on the application of Edward Bridges) v The Chief Constable of South Wales* [2019] EWHC 2341 (Admin) ("*Bridges*") ruled that automated facial recognition was justified as it had a lawful basis and the legal framework used by the SWP was proportionate. On lawful basis, the court referred to SWP's common law powers to keep the peace and prevent crime, legislation such as the Data Protection Act 2018 and the GDPR, the Surveillance Camera Code of Practice, and policy documents that provide standards against which the lawfulness of SWP's use of AFR Locate can be assessed. These enumerated legal powers whilst relevant, are not, however, specific on the use of FRT.

On proportionality, the court took note of the following points about AFR Locate and its use: (i) in the event of no match, the biometric data about the individual would be immediately deleted; (ii) AFR Locate was deployed with "significant public engagement" and used for a "limited time" and for a "limited purpose" to identify persons of "justifiable interest" to the police who may have been in the location; (iii) the alternative of installing more CCTVs was considered inadequate to achieve the aims of detecting crime and ensuring public safety; (iv) the targeted and limited scope of persons in the watch lists and the locations in which AFR Locate was deployed; and (v) the past results and benefits generated by AFR Locate in the making of arrests and searches for individuals by the police. Such considerations may also be applicable with adaptations to FRT use in public health surveillance.

The court relied on the above features and evidence to reject other grounds of challenges based on the breach of the UK Data Protection Act 1998, and the failure to comply with the Data Protection Act 2018 with regard to the sensitive processing of biometric data. SWP had also prepared a Data Protection Impact Assessment in discharge of its obligation under the 2018 Act.

On the question of bias, the court noted there was no evidence that the software generated results that suggest indirect discrimination with respect to the requirements under the Equality Act 2010. In any event, SWP had taken note of such requirements in issuing an Equality Impact Assessment in 2017.

A final important point is the court's pronouncement that questions of proportionality are fact-sensitive. The fact that FRT was adjudged to be proportional in that instance did not mean it would be permissible for criminal law enforcement or indeed for any health surveillance purposes. (Note: An appeal has been filed and a decision from the English Court of Appeal is pending.)

The European Commission has in its recent "White Paper on Artificial Intelligence – A European approach to excellence and trust" (19 February 2020) highlighted the risks for fundamental rights from the use of FRT and the need for safeguards subject to the requirements of proportionality, respect for the essence of the right to data protection and the necessity for processing of biometric data. Further, the GDPR states that processing of data concerning health is prohibited unless it is "necessary for reasons of public interest in the area of public health" (Article 9).

In addition to the abovementioned safeguards, considerations should be given to FRT use to advance the public health purpose during the COVID-19 pandemic and not thereafter. The justifications for the infringements of privacy via FRT can only apply for the duration of the pandemic. An additional safeguard pertains to the security of data captured via FRT. Similar to the use of FRT in public places, the retention of data derived from its use must be properly justified. The data should be encrypted to minimise the risks of hacking. Furthermore, we should enquire if a data subject should be allowed to challenge the findings of the government through FRT use that a particular person has, for example, flouted restriction orders during the COVID-19 pandemic.

In sum, the mediation of the triangular relationship amongst the major concerns of public health, personal privacy and bias against minority or marginalised groups would have to be carefully navigated. Whether and to what extent FRT can be used for public health surveillance during the pandemic – a question of balancing trade-offs and implementing appropriate safeguards - cannot be determined *in vacuo* but only within a specific context.