HUMPHREYS
LAW

Big brother state
here to stay?

Published: 6 April 2020

HUMPHREYS
LAW

We take a deep dive into whether automatic facial recognition technology has a place in society during unprecedented times

Produced by

Victoria Clement
Paralegal

Husna Grimes
Senior Consultant

In this issue

Introduction

In October 2019, we took a deep dive into the High Court judgment that challenged the use of automatic facial recognition technology ("AFR"). The judgment, handed down on 4 September 2019, found that the use of AFR by South Wales Police was lawful despite finding its use an infringement of ECHR Article 8(1).

Society seems conflicted. The British Police seem to consider the judgment to be an unofficial green light for AFR contrasting to protests against it from other governmental agencies. Prior to corona, the police view was by no means unanimous across the UK population.

As the coronavirus outbreak continues, more countries are looking at technology a means to fight it. The use of AFR in the months to come may determine whether it has a role in society and whether it is here to stay for the long run.

I. Global fight against COVID-19

BIG BROTHER AIDS IN GLOBAL FIGHT AGAINST CORONAVIRUS PANDEMIC

Governments are implementing draconian measures to reduce the speed and spread of the virus. In the United Kingdom, the government has introduced the Health Protection (Coronavirus) Regulations 2020 which introduces a handful of new powers and rights to the government and police. The legislation sets out powers for "medical professionals, public health professionals and the police" to "allow for detention of members of the public for 'screening, assessment and imposing any restrictions" to reduce the spread of the disease.

Other countries have gone further.

In Iran, the prime minster has unleashed cyber tech usually reserved for their country's counter terrorism activities. The country is now using state-level intel gathering tools to enforce quarantine measures and to track every movement of those who have tested positive for the virus.

The Chinese state, who are no strangers to such technology, have ramped up their use of AFR to help fight the disease. Cameras scan and track individuals from crowds and pick up those who are not wearing a mask or have a fever. Police have been armed with high-tech smart helmets which automatically scan individuals for a fever. The helmet will sound if someone with a fever is detected.

In other Asian cities, such as Hong Kong and Taiwan, governments are questioning fundamental civil liberties in their fight against the virus. Those returning to both cities are subjected to a mandatory home quarantine period of 14 days. To enforce such measures, the governments track their citizens' locations with a location-transmitting wristband, as well as tracking their phones via GPS, satellite and Bluetooth functions. Government officers ring those under quarantine up to twice a day and demand video calls to check if they are at home. Non-compliance with these regulations can result in an immediate prison term.

Back in the United Kingdom, Boris Johnson has made it clear the government "will rule nothing out" to suppress the spread of the disease.

The NHS are eager to use technology to fight the disease. The innovative arm of the NHS, the NHSX is co- organising a "hack from home" hackathon from the 4th April 2020 – 5th April 2020 to allow the best minds to come together to think of digital solutions to fight the virus. The emphasis is on developing applications where citizens volunteer their data to help track the virus, rather than "having people's data simply taken away".

I. GLOBAL FIGHT AGAINST COVID-19

The NHSX are working with other third parties to develop a "contact-tracing" application on a voluntary basis. The application is expected to make its debut sometime just before or after the lockdown ends. The application uses Bluetooth signals to detect other mobile phones in the vicinity and track the people they have come into contact with. If someone then tests positive for coronavirus, those who have been in close proximity with the patient will be notified and asked to self-isolate.

More worryingly, the government has been speaking with a number of mobile phone providers and big tech firms. It is believed the government is looking to collaborate with telecom providers to access the location data of mobile users and use the data to track their movement. However, the tracking will only be limited to monitoring mass movement and will not involve any individual tracking of mobile users.

Although Three, BT and O2 have all confirmed they are in talks with the government, no specific details of what is being discussed has been made public. The extent to which, if at all, this breaches the GDPR is unclear.

However, the British Health Secretary, Matt Hancock, tweeted last month "the GDPR has a clause excepting work in the overwhelming public interest. No one should constrain work on responding to coronavirus due to data protection law."

The Information Commissioner's Office ("ICO") has also given the government the go-ahead to legally use personal data from people's mobile devices to track their movement if it is useful in stopping coronavirus. The ICO further commented "the important thing is that data protection is not a barrier to sharing data" and that "we will continue to work alongside the Government to provide advice about the application of data protection law during these unprecedented times."

II. United Kingdom and automatic facial recognition technology ("AFR")

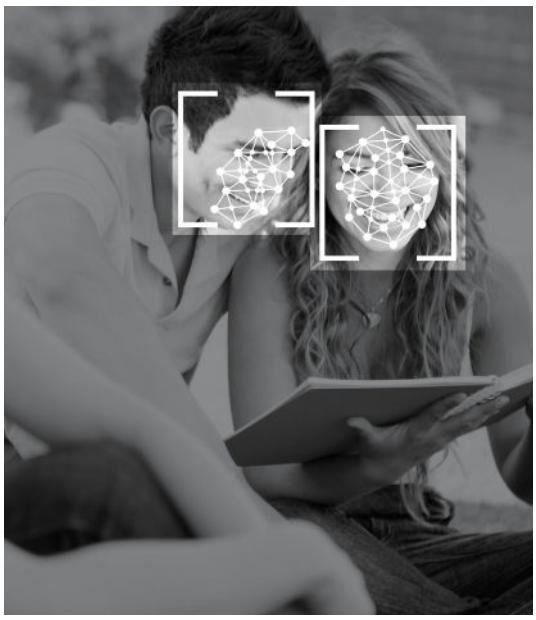
A. ICO'S INVESTIGATION INTO THE POLICE USE OF AFR TECHNOLOGY

On 31 October 2019, the ICO published its investigation into the police use of AFR. In conjunction, it also published the Information Commissioner's opinion on the technology. Elizabeth Denham, the Information Commissioner concluded that the current and future use of AFR is a regulatory priority for the ICO due to its invasive nature and infringement of human, information and data protection rights.

In the published opinion, she also called on the government to introduce a statutory binding code of practice to provide more safeguards on the use of AFR. Such a code would be helpful in informing different authorities about how and when AFR should be used.

She stressed the urgency of the implementation of such a code as it would offer law enforcement agencies "a highly desirable level of clarity and consistency."

She also strongly encouraged the police to make available information as to where AFR would be deployed, as well as let members of the public understand and check that their rights under data protection laws have not been violated.



II. UNITED KINGDOM AND AUTOMATIC FACIAL RECOGNITION TECHNOLOGY ("AFR")

B. HOUSE OF COMMONS – SCIENCE AND TECHNOLOGY COMMITTEE – BIOMETRICS COMMISSIONER AND FORENSIC SCIENCE REGULATOR (THE "COMMITTEE")

Earlier this year, the Committee concluded in their July 2019 report that the use of AFR by the police in various trials was concerning, given that there had been a "lack of independent oversight and governance of the use of AFR in these trials and recommended that, pending the development of a legislative framework, the police trials should comply with the usual standards of experimental trials, including rigorous and ethical scientific design".

As per their recommendation in their 2018 report, the Committee again recommended that AFR should not be deployed by the police in public spaces until issues with the effectiveness and accuracy had been resolved.

The Committee further referred to the *"regulatory lacuna"* that surrounded the use of AFR and called on the government to issue a moratorium until a comprehensive legal framework could be rolled out to govern the use of such technology.

II. UNITED KINGDOM AND AUTOMATIC FACIAL RECOGNITION TECHNOLOGY ("AFR")

C. BRITISH POLICE'S USE OF AFR

After the High Court judgment ruled AFR legal, the Metropolitan Police have fully embraced the technology. This is amidst a background of various human rights watchdogs protesting its use to be a fundamental violation of human rights. Various governmental bodies have also raised concerns about whether the police truly the authority have to deploy such technology.

In late January 2020, the Metropolitan Police force announced AFR would be used on the streets of the UK. It said the cameras would be used to scan the streets for people who were suspected of more serious crimes, such as child abuse cases and violent knife crimes.

Such a decision comes after ten trials of the technology across the city since 2016. The first trial of such technology had been deployed at the Notting Hill carnival back in 2016.

The first live use of AFR was deployed in Stratford in mid-February 2020, where vans with cameras mounted on them have sat outside Stratford station scanning the masses that walked past to pick up whether any faces matched with the 5,000 faces in the police's database.

The cameras failed to identity anyone of interest in the first four hours of deployment, despite hundreds of the public walking past.

Public outcries against the technology have been ignored, and people are getting creative in combating the deployment of the AFR cameras around London. A group of artists, the Dazzle Club, organises a monthly protest where they paint their faces with make up in an attempt to confuse the cameras and the data it collects.

Nevertheless, the Metropolitan Police force are confident of their AFR's accuracy, citing a 1 in 1,000 person false positive.

II. UNITED KINGDOM AND AUTOMATIC FACIAL RECOGNITION TECHNOLOGY ("AFR")

Such figures are starkly contrasted to the data released by an independent review investigation commissioned by the Metropolitan Police force, which estimates the technology was only 19% accurate.

The independent investigation was carried out by the University of Essex. They further concluded that the technology's algorithm was biased, and that it not did perform equally when processing different faces across age, gender and ethnicity.

The reason for so much discrepancy in how accurate the technology is lies in a number of factors. These include how proximate the cameras are from the individuals they are tracking, the network on what the data is fed back and the speed of the internet connection and whether it uses a 4G or 5G network.

III. European Union and AFR

EU GETS COLD FEET ON FIVE-YEAR BLANKET MORATORIUM ON USE OF AFR TECHNOLOGY

In February, the European Commission ("EC") retracted their plans to impose a five-year blanket moratorium on the use of AFR in public spaces. In their initial white paper published in mid-January, they had previously considered imposing a five-year ban on all use of all AFR, where they had hoped member states would use the time between to study and assess the impact of AFR if rolled out across society.

The EC white paper focussed on a European approach to the use of artificial intelligence, and discussed the use of AFR. It stressed the importance of member states and private bodies to respect the EU's General Data Protection Regulation, which give citizens "the right not to be subject of a decision based solely on automated processing, including profiling."

In a later draft, published on 19 February 2020, the EC removed the five-year blanket ban on the use of AFR technology. Instead, it left the decision of whether AFR should be used to each individual member state. It did, however, reiterate its concerns over the inaccuracy of AFR technology and its potential breach of data protection laws.

IV. Other perspectives

A. THOUGHTS FROM A COMMERCIAL PERSPECTIVE

Most governmental agencies seem to have concerns about AFR – but what about businesses already using it?

We spoke with Richard Hicks, co-founder and COO of C-Screens Ltd, the UK's largest out-of-home ("OOH") TV network.

His business uses AFR to track out-of-home TV viewers that are engaged with their screens in busy popular pedestrian areas and consumer entertainment environments. The audience data includes approximate number of views, age and gender tracked in real time. All data collected are binary and anonymous. This key first party data is fed back to brands who are trying to invest in adverts that can reach "the right audience, with the right advert, with relevant premium programming, in the right environment".

Hicks lamented the lack of practical and digestible guidance regarding the commercial use of such technology given by the ICO. Although Hicks is confident that his business is GPDR compliant, the lack of governance or guidance given by any governmental agency means it is left entirely up to companies that use AFR to govern themselves. Without any codified guidance written specifically for the commercial use of AFR, smaller businesses are left to navigate the myriad of various legislation that come together to govern the use of such technology. "We would be more than happy to work with leaders to help govern this space."

Without much official guideline on the use of AFR and the ICO considering a ban on AFR, Hicks' business operates on a 'wait and see' approach to the use of the technology. Until then, businesses that use such technology can either engage their own compliance experts out of pocket or turn to various industry bodies for further guidance. For example, those involved in the advertising space have turned to the Internet Advertising Bureau, the industry body for digital advertising, or Outsmart, the marketing body for the OOH industry. These non-governmental agencies now act as the first point of call for smaller businesses who are concerned about compliance issues with the use of AFR technology.

IV. OTHER PERSPECTIVES

B. THOUGHTS FROM A UK DATA PROTECTION/PRIVACY PERSPECTIVE

Given the potential for technological bias and concerns that this may lead to discrimination when using AFR technology, this is where data protection by design and default really comes into play. By following privacy by design principles, which have been around pre-GDPR so are by no means new, these issues would be addressed and mitigated right from the design stage and throughout the AFR technology's lifecycle.

We would have expected the Metropolitan Police force's data protection impact assessment to consider and address all of the issues in the University of Essex's report at the start of the project – e.g. identifying the risk of bias, how they planned to approach this, and their proposed steps to mitigate against discrimination and ensure that appropriate safeguards and technical measures could be put in place throughout the project build phase.

Clearly this is a complicated area to navigate and data protection regulators are still catching up as they work to produce much-needed guidance to help organisations utilise this technology responsibly within the regulatory landscape.

With that in mind, it is even more important to establish good privacy by design practices from the outset and engage internal and external support from subject-matter specialists who have the relevant expertise to advise on how AFR technology should be designed, tested and implemented.

Husna Grimes,
data protection specialist
at Humphreys Law

V. Final Thoughts

AFR technology has long had a sinister reputation for its potential breach of civil liberty rights, but the virus has now presented a new justification for the widespread use of such technology in society – the protection of public health. As the coronavirus pandemic unfolds, this is a once in a lifetime opportunity for AFR to be trialled and tested to discover if it truly lives up to its bad reputation, or whether there is a useful place for it in our societies.

The issue of whether the Metropolitan Police force's use of AFR is justified and whether other governmental agencies will have to come to accept that AFR's place in modern society will be further clarified when the appeal of the High Court case that triggered all of this is heard. Until then, different governmental agencies will be stuck in limbo as they try to balance the pros and cons of the use of AFR.

This piece was researched and prepared by Victoria Clement with input from Husna Grimes of Humphreys Law and Richard Hicks from C-Screens Ltd, a client of Humphreys Law.

All the thoughts and commentary that HLaw publishes on this website, including those set out above, are subject to the terms and conditions of use of this website. None of the above constitutes legal advice. None of the above should be relied upon. Always seek your own independent professional advice.

About **Humphreys Law**

Humphreys Law is a full-stack law firm for media and tech. We advise companies of all sizes, and investors of every kind, on high stakes transactions and complex projects.