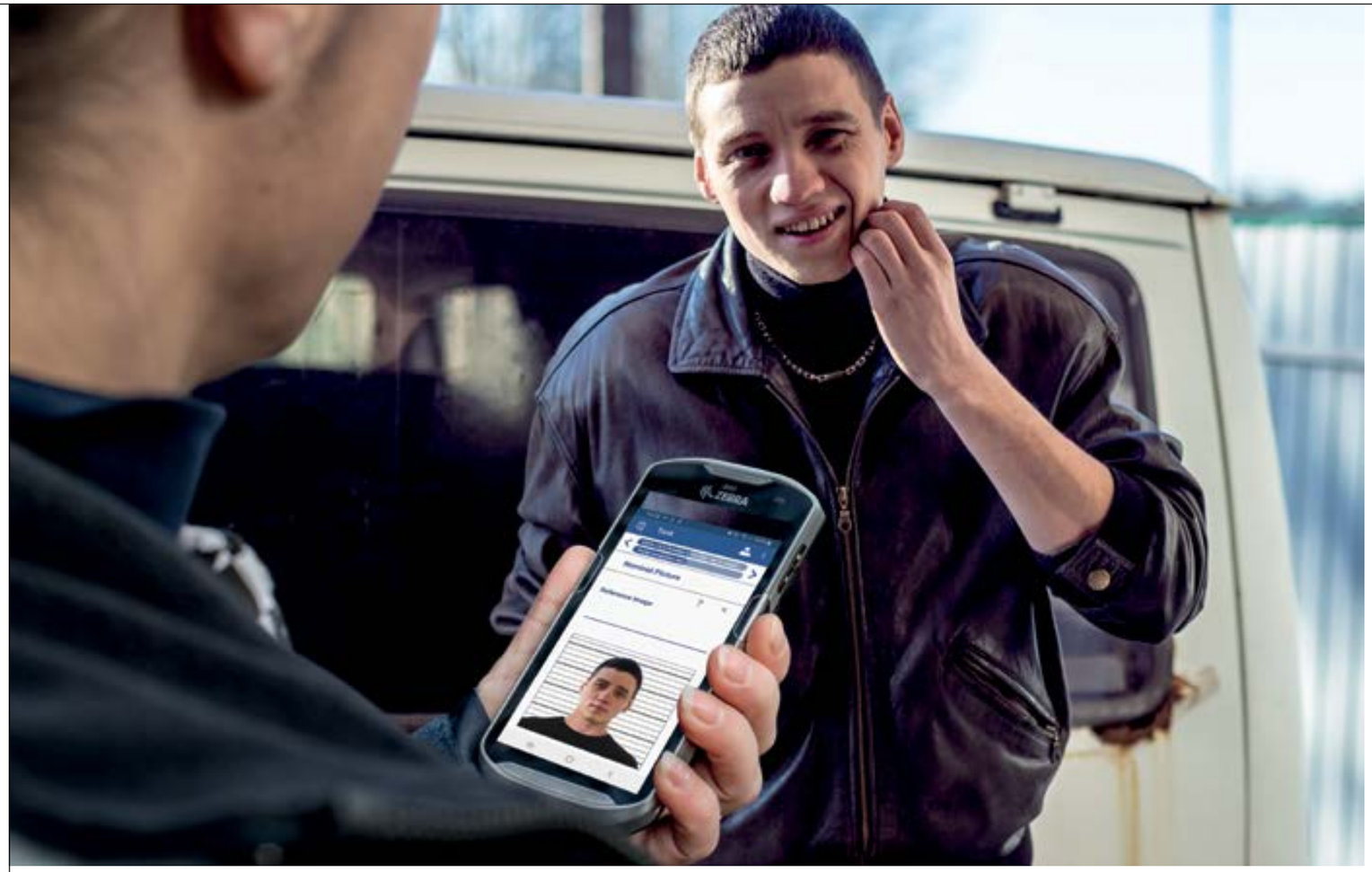


Picture credit: Coeus Software

FACIAL RECOGNITION

Simon Hall *examines why emerging technology is a good thing for policing, although it's vital that it is closely monitored*

In January *The Independent* newspaper exclusively revealed that the Metropolitan Police had spent over £200,000 on facial recognition trials throughout the capital. According to the details obtained from the freedom of information request, the Met had conducted six facial recognition trials by that time, resulting in two people being stopped and later released. No arrests were made as a result of the trials.

The tone of the article was somewhat critical suggesting: "UK's largest police force spends over £200,000 on facial recognition trials that resulted in no arrests". The implication being that with no arrests as a result of these trials, the authorities were wasting public money. Some sources were quoted as describing the force's use of facial recognition as a "shambles".

While continuing to face criticism from privacy groups, the Met has not ceased its trials. According to *ComputerWeekly*, its ninth trial took place in Romford town centre on 31 January. This time eight people were arrested during the eight-hour deployment, of which three were as a direct result of the technology identifying individuals who were wanted in connection to violent offences. One of them, a 15-year-old boy, was later released without further action. Is the Met right to be trialling facial recognition technology in the wild? Why is the technology so controversial? And do the benefits really outweigh the potential drawbacks?

Facial recognition can be used to quickly verify if a person is who they claim they are

It is all too easy to criticise the police for using facial recognition technology on civil liberty grounds. It is a very emotive topic, which for many can conjure up images lifted straight out of Orwell's dystopian classic, *1984*. But if Orwell has taught us anything, it's that his fiction can sail very close to the wind. In China, for example, facial recognition technology is already widely used in the commercial sector for checking into airports, withdrawing cash and making purchases from vending machines, restaurants, shops *etc*. But it is no secret that the Chinese Government is also exploring plans to develop a national surveillance system directly based on facial recognition, which could be used to monitor not just the behaviour of its 1.4 billion citizens, but an almost limitless amount of other factors from their emotional state to their sexuality. It is here where the fears expressed by civil liberty groups are perfectly rational and go far beyond reciting the fears of historical fiction.

POLICING BY CONSENT

Taking these genuine concerns to one side, any technological development which has the potential to transform the *modus operandi* of any discipline should always be closely monitored and scrutinised. Facial recognition is no exception to this. But even more caution is necessary when this discipline happens to be the police service. We must be cognisant that any change in police tactics does not undermine the core tradition of *Policing By Consent*, the nine principles of policing that have been issued to every new police officer since 1829. With this in mind, however, this does not mean we should necessarily stifle the development of facial recognition in the police, but we should pay close attention to it. You cannot put the genie back in the bottle. Facial recognition, and more broadly AI, is here to stay. The question now is what do we do with it? This can only be determined by further development, testing and monitoring. From this perspective, and with legitimate concerns always front of mind, the Met and other police forces are right to be testing facial recognition in limited trials prior to any more significant deployment.

We should also remember that this is not an easy technology to develop, so it is important for forces to trial it in order to enhance its effectiveness and address any public concerns before wider adoption is even considered. We should view it as a positive step that the police are open to trialling any new technology solutions that may ultimately be crucial in keeping the public safe.

Facial recognition is a subset of Artificial Intelligence (AI), so it is important to look at in this broader technological context. The AI industry is still very much in its infancy, but it has the potential to transform every industry for the better. The fundamental benefit of AI is its ability to draw conclusions and highlight trends from highly complex data sets. There are many ways in which this could be leveraged by the police to prevent and solve crimes, beyond just facial recognition. In crime prevention for example, it can be used to determine patterns of criminal behaviour to improve the chances of catching criminals in the act (eg finding patterns in a spate of burglaries or predicting the destination of a high-speed pursuit). In crime solving AI can be used to spot correlations in evidence which were otherwise missed by detectives in a murder investigation. In both examples AI supports and enhances the existing police function; but crucially it does not replace the decision-making capability of the human police officer.

AI can potentially make limited decisions on behalf of the police, but we believe these will and should always be limited in scope. An AI system could, for example, make intelligent recommendations as to who an officer should stop and search in order to find offensive weapons during higher-risk events such as at sports tournaments or music concerts. In this scenario the AI is making limited decisions in very specific circumstances, but the ultimate decision remains at the discretion of the officer. Facial recognition technology has huge potential for improving public safety, particularly when combined with other data sources (gait recognition, clothing colour *etc*.) to help identify suspects in large crowds. An AI engine can analyse hundreds of data points far more quickly, effectively and discretely than a team of officers could ever do. With the right checks and balances, this can be a real force for good.

DEALING WITH CONCERNS

There is no escaping the very valid civil liberties concerns which need to be ironed out before any UK police force can use facial recognition at any scale (whether on a one-to-one basis or in mass surveillance). Like any tool, the way facial recognition technology is used will significantly affect its effectiveness and its impact on civil liberties. There are three major concerns here: false positives causing innocent people to repeatedly become suspects, false negatives – where people of interest are not detected – and the widespread tracking of individuals without their consent or knowledge.

The first two concerns are largely technological in nature. They are not arguments against trials, but for them. The only way to iron out the kinks in a technology is to test it in real-world scenarios. Much like self-driving cars need real-world data to improve their understanding of the real world, and for that they need to drive on public roads, facial recognition needs test data from real faces in real-world scenarios.

AI CAN ANALYSE DATA FAR MORE EFFECTIVELY AND DISCRETELY THAN A TEAM OF POLICE OFFICERS

The third concern is less a technological challenge, but a legislative and regulatory one. This is where *Policing By Consent* becomes relevant. We have to ask the question: does facial recognition technology have the public's support? Does it undermine the principles of policing by consent? The point is that, much like automatic number plate recognition can track vehicles, facial recognition can track people. But the crucial difference between number plate and facial recognition is that we can choose whether to drive a vehicle and abide by the associated rules (we therefore choose to give our consent when we get

into the vehicle), but we have no such choice when it comes to facial recognition. There is no opt out for facial recognition in public spaces. In the wrong hands it could become a tool of harassment or even persecution. Its use and development, therefore, needs to be closely monitored.

When used as a mass screening tool, biometric technologies are more likely to throw up false positives; every person passing in the camera's field of view is checked against every person in the database, whether that individual is of interest or not. If, say, there are 100,000 people in the database and 10,000 people are screened, that's one billion potential comparisons, so the false positive rate has to be extremely low to prevent false matches. Clearly identification cannot rely on facial recognition alone. Additional data sources are also necessary.

FACIAL RECOGNITION TECH HAS HUGE POTENTIAL TO HELP IDENTIFY SUSPECTS IN LARGE CROWDS

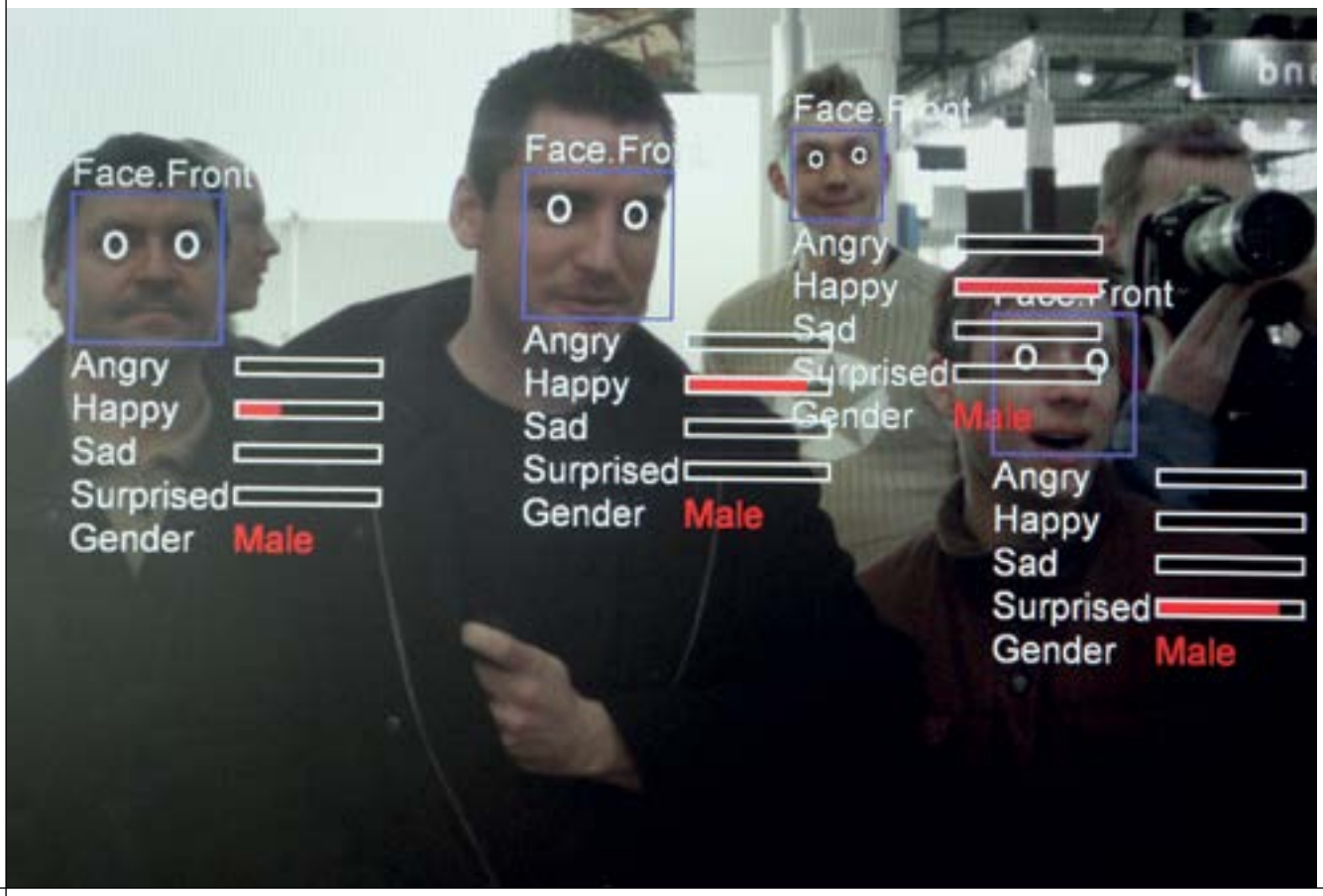
Facial recognition and other biometric technologies can be more effective when used in a narrower context, such as verifying if someone is who they claim to be (in which case the check would be against a single record, not the entire biometric database), or carrying out checks on someone where the officer already has reasonable grounds to suspect that person of an offence. This is the approach taken with the biometric capabilities of PoliceBox, for example, the mobile working solution for front-line officers. In these cases, the number of comparisons being performed is much lower and, therefore, the chances of false positives is correspondingly lower. What's more, as the subject is directly involved in the process by interacting with the officer, this also gives them the opportunity to give informed consent for the check where appropriate – or at least to be aware that the check is being performed. Such use of facial recognition does not contradict with the notions of *Policing By Consent*.

BENEFIT TO SOCIETY

Clearly there are cases where the mass-scale use of facial recognition and other machine-based analysis can be of clear benefit to society, such as the investigation or prevention of terrorist incidents. Thousands of hours of CCTV footage can be analysed quickly and clips of potential interest can be flagged for human inspection. Used in this way as a supporting tool, the technology could accelerate the identification, location and arrest of suspects before they can cause further harm. But it is important that the use of facial recognition remains in step with public perception. It is important for the trials of the technology not to run beyond what is considered acceptable by the public.

What is currently missing is a strong regulatory framework whereby, with certain exceptions such as ports of entry, the general use of facial recognition screening data without informed consent can only be authorised under very specific conditions through an appropriate, impartial process. The technology should continue to be developed and tested in small-scale trials, but legislation that pays close attention to the nine principles of policing (particularly with regards to consent and the need for public approval and respect) needs to be in place to safeguard the public before it is adopted on any national scale ●

Simon Hall, CEO, Coeus Software, the developer of PoliceBox and Quvo – two cloud-based, mobile workforce services for the police and other sectors.



Facial recognition can be used for more than just identifying criminals

Picture credit: Getty