Northumbria University NEWCASTLE

Feb 09, 2018 11:24 GMT

EXPERT COMMENT: Police mugshots: millions of citizens' faces are now digitised and searchable – but the tech is poor

Martin Paul Evison, Professor in Forensic Science at Northumbria discusses digitised Police mugshots for The Conversation.

The steady march of technological progress has finally shone its light into the dingy world of the mugshot – the commonplace name given to the photograph of a police suspect.

The mugshot represents one of the earliest uses of technology in the identification of criminals. It has proved to be a particularly useful way of identifying recidivists – people who repeatedly reoffend.

Its adoption in France in the mid-19th century meant that by 1872 – only 40 years after the abolition of branding – the Parisian authorities were making comparisons of daily arrestees with 60,000 accumulated photographs.

Unhelpful inconsistencies in photography led to the implementation of standard anterior and lateral profile photographs taken at one-seventh scale – a convention that hasn't changed in more than a century, even following the introduction of digital photography.

Dermatoglyphic fingerprinting and, ultimately, DNA profiling have offered more reliable forms of forensic human identification, but identifying faces remains critical in recognising suspects.

Police in England and Wales – using photo recognition technology – have now accumulated millions of images of people, many of whom may never have been charged with or convicted of any offence.

The case of S and Marper versus the UK in the European Court of Human Rights drew attention to the issue of retention of DNA samples and profiles of people who had never been convicted of an offence. It led to the UK systematically disposing of arrestee DNA and dermatoglyphic fingerprint evidence in routine cases not proceeding to a charge.

Don't smile, please, you're on camera

But what about the mugshots? These are no longer stored solely in an album on a dusty shelf in the corner of a local police station, but are digitised and searchable – and imminently there will be a capability for national remote database interrogation.

Use of public area CCTV has burgeoned and the camera's seemingly universal presence has led to vocal objections from activists and some academics.

Others have drawn attention to the benefits, however, and security cameras are widely accepted by the public. Their value in criminal investigation is unquestionable – over 3,000 suspects were recognised by eyewitnesses from footage examined following the London riots of 2011.

There are also dangers associated with the automatic computerised searching of CCTV video streams for people depicted in arrestee photographs. Should the mugshot databases be purged in much the same way that DNA and fingerprint ones are?

Public area computerised facial recognition has been just around the corner for decades – and still is. It's worth noting that only one suspect in over 3,000 from the London riots was recognised by computer software and an attempt by "digilantes" to identify suspects by matching them to social media images held on the web failed.

The story of facial recognition software being used to identify a suspect at the 2017 Notting Hill Carnival was a similar debacle. That particular attempt apparently led to a number of false positive matches and people mistakenly being stopped by police. In contrast, South Wales Police have claimed a number of arrests using similar technology.

But in the absence of independently controlled studies, considerable doubt remains regarding in what circumstances, if any, the technology is ready for face-in-a-crowd applications. People – like the Metropolitan police's "super-recognisers" – perform infinitely better and, oddly, don't seem to attract the attention of activists.

Removing people who were arrested but never charged from police fingerprint and DNA databases exemplifies the uncertain consequences of dogged social action. The theoretical risk of a person who was never charged being associated with a crime scene they were never at has been reduced. However, it has also introduced the perverse certainty that they will not be associated with a crime scene where they were present.

Probability dictates that detection will have been missed – including in serious offences – simply because the database is smaller; although repeat offenders do predictably find their way onto the system.

Both the House of Commons science and technology select committee and the Biometrics Commissioner, Professor Paul Wiles, have expressed concerns about the delay in publication of the Home Office's heavily delayed biometrics strategy. Home office minster, Baroness Williams, stated recently that it will be published in June this year.

This is anticipated to be a combined forensic and biometric strategy, following the poorly-received Home Office forensic science strategy of 2016, which was heavily criticised by MPs. This is likely to be a big challenge for the Home Office, which is ill-equipped with the breadth and depth of scientific and technological know-how needed to inform these strategies, and must inevitably rely on advice from parties unlikely to be impervious to influence by commercial or other self-interest.

The compulsion is to give everything to the police, who are hardly any better placed – as the Notting Hill Carnival problems show – and for whom biometrics and forensics are far down the list of priorities, following massive budget cuts and political and media pressure to prioritise certain types of crime, despite a questionable evidence base.

The government's combined strategy needs to focus on the effectiveness of those biometrics that are reliable and on the contexts in which they work best – typically fingerprints, DNA and irises. Despite the claims of its

proponents, biometric technology doesn't work very well in real-world situations, presenting risks of over-reliance and unjustified alarm. For these, light touch regulation – such as guidelines subject to review – is sufficient.

Eyewitness facial identification – especially of unfamiliar faces – is not reliable given that it underlies many serious miscarriages of justice. And facial recognition technology performs extremely poorly in public areas.

The pruning of the fingerprint and DNA databases at the hands of well-meaning civil liberty activists has led to two of the most reliable forms of forensic human identification being displaced by one of the least. It's yet another perverse result for those interested in promoting reliable biometric and forensic identification to help the police do their job.

This article was originally published on The Conversation. You can read the original article here.

Contacts

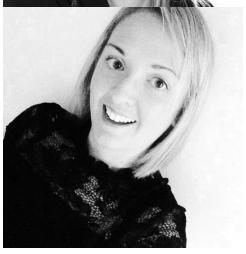
Rik Kendall
Press Contact
PR and Media Manager
Business and Law / Arts, Design & Social Sciences
rik.kendall@northumbria.ac.uk
07923 382339

Andrea Slowey
Press Contact
PR and Media Manager
Engineering and Environment / Health and Life Sciences
andrea.slowey@northumbria.ac.uk
07708 509436

Rachael Barwick
Press Contact
PR and Media Manager
rachael.barwick@northumbria.ac.uk
07377422415

James Fox
Press Contact
Student Communications Manager
james2.fox@northumbria.ac.uk

Kelly Elliott
Press Contact
PR and Media Officer
kelly2.elliott@northumbria.ac.uk



Gemma Brown
Press Contact
PR and Media Officer
gemma6.brown@northumbria.ac.uk