The background features abstract, overlapping geometric shapes in various shades of blue, ranging from light sky blue to deep navy blue. The shapes are primarily triangles and polygons, creating a dynamic, layered effect. The text is centered on a white background that is partially framed by these blue shapes.

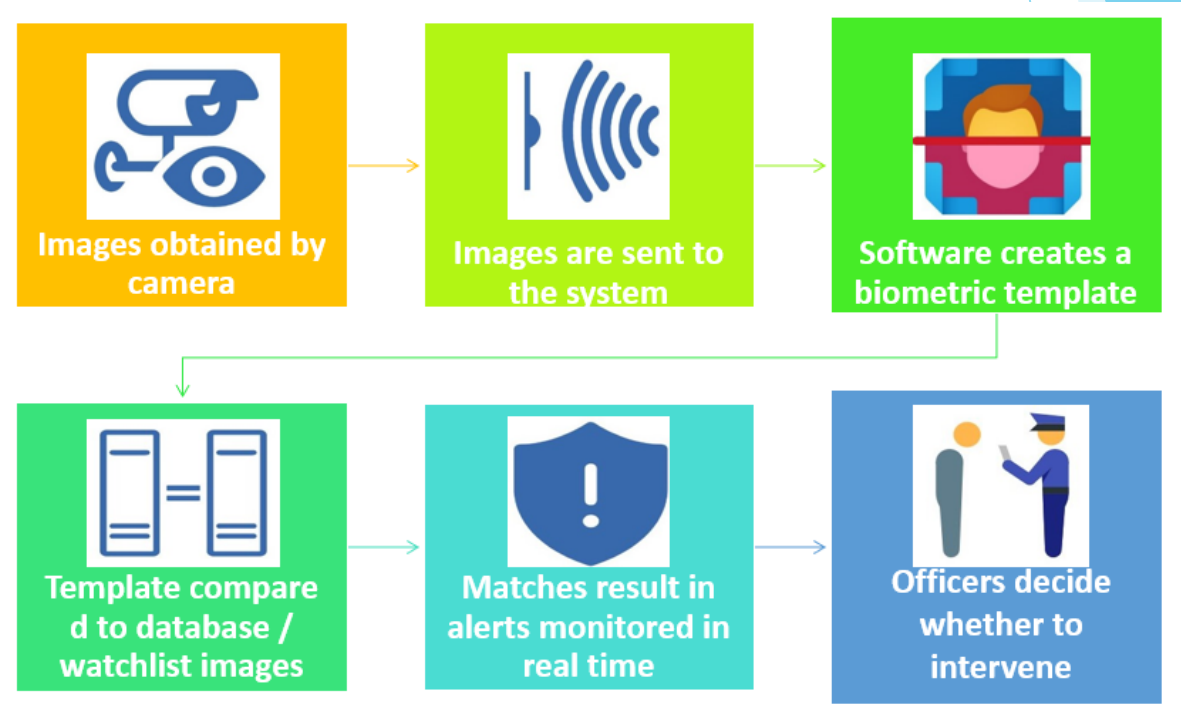
An analysis of the development and use of live facial recognition technology by law enforcement in the UK and its impact on adequacy

Presented 17th Sept 2021

Dr Allison M Holmes

Background and Context

- ▶ Focus is on ‘Live Facial Recognition’ in publicly accessible spaces
 - ▶ England and Wales
- ▶ *Can the issues presented in LFR could represent a ‘serious and systemic’ deficiency as regards the principles of the rule of law which could impact on the adequacy agreement?*



Questions of Adequacy

- ▶ Law Enforcement Directive 2016/680 Article 36 provides a decision may be reached whereby a third country provides an adequate level of protection
 - ▶ Facilitates information sharing between EU and that third country
- ▶ Commission Implementing Decision of 28 June 2021 pursuant to Directive (EU) 2016/680 of the European Parliament and of the Council on the adequate protection of personal Data by the United Kingdom
 - ▶ Article 3
 - ▶ 3(3) : The Member States and the Commission shall inform each other of any indications that interferences by United Kingdom public authorities with the right of individuals to the protection of their personal data go beyond what is strictly necessary, or that there is no effective legal protection against such interferences.
 - ▶ 3(4): Where the Commission has indications that an adequate level of protection is no longer ensured, the Commission shall inform the competent United Kingdom authorities and may suspend, repeal or amend this Decision

In 'accordance with law' in the UK

Common Law
Powers

Data Protection
Act 2018

GDPR

Surveillance
Camera Code of
Practice

Equality Act
2010

Human Rights
Act 1998

Protection of
Freedoms Act
2012

Bridges v CC South Wales Police [2020] EWCA Civ 1058

Box 1: The legal issues in the use of live facial recognition by South Wales Police identified in the *R. (Bridges)* case

| | |
|---|--|
| 1 | The use of the automated facial recognition (AFR) system was held to have breached the right to respect for private life protected by the UK Human Rights Act 1998 because the court found critical defects in the legal framework that left too much discretion to individual officers. |
| 2 | The AFR system had breached Section 64 of the Data Protection Act 2018 on the basis that the Data Protection Impact Assessment had <i>“failed properly to assess the risks to the rights and freedoms of data subjects and failed to address the measures envisaged to address the risks arising from the deficiencies we have found”</i> . This included two <i>“impermissibly wide areas of discretion”</i> ; the selection of those on watchlists; and the locations where AFR may be deployed. |
| 3 | South Wales Police (SWP) was in breach of its public sector equality duty (PSED) under section 149 of the Equality Act 2010 in that <i>“SWP have never sought to satisfy themselves, either directly or by way of independent verification, that the software program in this case does not have an unacceptable bias on grounds of race or sex”</i> . |

EU Legislative Position and Developments

- ▶ Directive 2016/680
 - ▶ Recital 33 - 'rules of national law'
 - ▶ Article 10 - biometric processing
- ▶ Proposed European Artificial Intelligence Act
 - ▶ *Lex specialis*
 - ▶ Article 5
- ▶ EDPS & EDPB criticism

Watchlists: England and Wales v EU

Position

England and Wales

- ▶ Lack of statutory framework
- ▶ College of Policing APP proposed guidelines for use of LFR
 - ▶ Wanted by the courts
 - ▶ Suspected of committing an offence/
reasonable grounds to suspect
 - ▶ NB: no level for the offence
 - ▶ Subject to bail conditions
 - ▶ Presenting a risk to harm of themselves or others
 - ▶ Victims or witnesses to offences
 - ▶ or close associates who would fall under any of these categories

EU AI Act

- ▶ Act provides an exhaustive list of use of LFR in publicly accessible spaces
- ▶ Targeted searches for specific potential victims of crime, including missing children
- ▶ Prevention of a specific, substantial, and imminent threat to life or physical safety of natural persons or a terrorist attack
- ▶ Perpetrator or suspect who commits one of 32 categories of offences listed in the Framework Decision on the European Arrest Warrant

Watchlists: ‘Strict Necessity’

- ▶ Seriousness of offences ; high threshold for inclusion
- ▶ Limited in size/scope
- ▶ Image quality
 - ▶ Images of uncertain provenance
 - ▶ Custody images
 - ▶ S 64A PACE 1984
 - ▶ R (RMC and FJ) v Commissioner of Police for the Metropolis and Secretary of State for the Home Department [2012] EWHC 1681
 - ▶ Gaughran v UK (2020)
 - ▶ Age of images and associated metadata
- ▶ Inclusion of ‘non-police originated images’
 - ▶ Communication on the EU Security Union Strategy published by the Commission on 24 July 2020 calling inter alia for a modernisation of the Prüm Decisions

Oversight of Use

England and Wales

- ▶ Deployments authorised by an ‘Authorising Officer’ of at least the rank of Superintendent
 - ▶ Derogations in cases of emergency
- ▶ College of Policing APP requires chief officers establish their own ‘internal governance procedures’
- ▶ Internal oversight bodies
- ▶ Ethics panels
- ▶ Biometrics and Surveillance Camera Commissioner

EU

- ▶ Pre-authorisation by judicial authority or independent administrative authority
- ▶ Position favoured by the CJEU jurisprudence

Future Concerns and Conclusions

- ▶ Expansion of public-private collaborations in the use of LFR
- ▶ Increase in similar technologies in the absence of statutory frameworks
- ▶ Indicative of diverging standards between UK-EU in the area of law enforcement data processing

Questions

Contact: a.m.holmes@kent.ac.uk