CRITICALLY ENVISIONING BIOMETRIC ARTIFICIAL INTELLIGENCE IN LAW ENFORCEMENT

FINAL PROJECT REPORT

UKRI Engineering and Physical Sciences Research Council
UKRI Trustworthy Autonomous Systems Hub
THE UNIVERSITY of EDINBURGH Edinburgh Law School
UKRI Research Node on TAS Governance & Regulation
UNIVERSITY of STIRLING

CONTENTS

INTRODUCING THE TEAM & ACKNOWLEDGEMENTS

Overall Project Lead – Dr Lachlan Urquhart

Dr Urquhart is a Senior Lecturer in Technology Law and Human-Computer Interaction, University of Edinburgh. He is a Director in both the Scottish Research Centre for Intellectual Property and Technology Law (SCRIPT) and the Centre for Research on Information, Surveillance and Privacy (CRISP). He is founder and Director of the Regulation and Design Lab. He has a multidisciplinary background in computer science and law and has published 55 papers in leading venues in computing, law, and ethics. He has been a lead and co-investigator on projects totalling over £6m from EPSRC, ESRC, AHRC, and he is currently Principal Investigator of the EPSRC £1.2m 'Fixing the Future: Right to Repair and Equal-IoT' project and Co-Investigator on the ESRC Emotional AI in Smart Cities project, EPSRC Trustworthy Autonomous Systems Governance Node, and on various projects in the EPSRC Horizon Trusted Data Driven Products hub.

Co-Lead – Dr Diana Miranda

Dr Miranda is a Lecturer in Criminology in the Faculty of Social Sciences, University of Stirling. Previously, she held teaching and reseach positions in several universities in the UK (The Open University, Birkbeck - University of London, Keele University, Northumbria University) and Europe (Portugal and Spain). She is a member of CRISP (Centre for Research on Information, Surveillance and Privacy), SCCJR (Scottish Centre for Crime and Justice Research) and SIPR (Scottish Institute for Policing Research). Her research aligns criminological and sociological approaches to explore emerging biometric, and data driven, surveillance technologies. She has published over 20 journal articles and book chapters and given over 40 academic talks. She is a Co-Investigator on the ESRC Emotional AI in Smart Cities project.

Lead Author of Systematic Literature Review – Dr Irena Connon.

Dr Irena Connon is a Lecturer in Social Sciences at the University of Stirling who has previously held positions at the University of Edinburgh, University of Dundee, and the University of Technology Sydney. She is a Social Anthropologist and transdisciplinary researcher whose research focuses on understanding differentiated experiences of environmental hazards and disasters; enhancing the inclusion of marginalised people in Disaster Risk Reduction activities; climate and environmental risk perception, communication, and management; and, more recently, the social, ethical, and legal implications of emerging technologies and AI in society. Her research has been published in international peer-reviewed journals and has been used to inform policy and practice in Scotland, the wider UK and Australia. She is a member of the Regulation and Design Lab (RAD) and has served as a consultant for the Scottish Parliament.

Lead Creator of Design Fictions – Dr Alexander Laffer

Dr Laffer is a Lecturer in Media and Communication, University of Winchester. Previously, as a Research Fellow at University of Edinburgh and at the Emotional AI Lab, Bangor University, he has worked across numerous projects exploring the ethics of implementing emergent technology in a range of personal, civic, and security contexts. He is a member of the Regulation and Design Lab (RAD). His research is in the areas of Discourse Analysis, Digital Media and Empathy, with a current focus on Emotional AI, Design Fictions and the affordances of new narrative forms. He has published across media and linguistics as well as creative pieces, which he uses to further explore research concerns.

Acknowledgements:

This research is supported by funders EPSRC TAS Hub [EP/V00784X/1]; TAS Governance and Regulation Node [EP/V026607/1] and ESRC Emotional AI in Smart Cities Project [ES/T00696X/1]. Thanks to our attendees at the Roundtable on March 23rd, 2023, from: The Scottish Biometrics Commissioner; Information Commissioners Office; Scottish Policing Authority; Scottish Government; University of Edinburgh; Stirling University; and Bangor University. Thanks to University of Edinburgh PhD Students Ayça Atabey for help on the day and to Sarah Ahmad for Graphic Recording and Final Report Design.

PART 1. INTRODUCING THE PROJECT

PART 1. INTRODUCING THE PROJECT

This report presents an overview of the **Critically Exploring Biometric AI Futures** project led by the University of Edinburgh in partnership with the University of Stirling. This short 3-month project explored the use of new Biometric Artificial Intelligence (AI) in law enforcement, the challenges of fostering trust around deployment and debates surrounding social, ethical and legal concerns. The Report includes a discussion of:

- A **Rapid Systematic Review** of existing scholarly and policy-relevant literature focusing on emerging biometric AI technologies in Law Enforcement and the social, ethical, and legal issues that have been associated with these tools.
- The **Creation of 3 Design Fictions**, drawing on the Review, to explore emergent uses of Biometric AI in Law Enforcement. These broadly consider law enforcement uses of Live Automated Facial Recognition; Emotion Recognition; and DNA Phenotyping
- A **High-Level Expert Roundtable** run with Key Stakeholders in Policing at the University of Edinburgh (e.g., academics, policing professionals, regulatory body members, Government representations). This Roundtable was graphic recorded.
- A **Summary** of Discussions at Roundtable Discussions.

This work builds on prior research conducted by the project team on AI, policing, biometrics, and regulation, such as: Laffer, Urquhart, and Miranda in the ESRC Emotional AI Project e.g. (Urquhart and Miranda 2022; Urquhart, Miranda and Laffer 2022; Laffer 2022); Connon and Miranda in the Emergent Technologies in Policing Project (Connon et al 2023); Miranda in the Body Worn Video Project (Webster, Miranda and Leleux 2022); and Urquhart in the TAS Governance Node e.g. (Urquhart, McGarry and Crabtree 2022).

Biometric AI involves technologies making automated inferences about the body through analysing physiological, behavioural, and biological traits. To function, AI systems take inputs [such as data from an environment] and use techniques [such as machine learning] to generate outputs [such as assessments and inferences based on the data]. For Biometric AI, this involves processing inputs like facial features, human micro-expressions, body language, movement, gait, fingerprints, voice, and genetic DNA material. Outputs are not focused on identification purposes only but also to make inferences about or categorise the subject e.g., emotion recognition or gait analysis (McStay and Urquhart 2019; Ryder 2022). There is significant complexity in generating outputs, depending upon the volume, variety, and variability of data involved in training models (Information Commissioner's Office 2023). Further, there are often concerns around the provenance, completeness, bias, and potential errors in this data. With policing, the oversight and legality in sourcing datasets become a greater concern, particularly as consequences of misuse can impact trust relations between the police and citizens (Urquhart and Miranda 2022). The nature of how the model is trained, such as if it uses supervised or unsupervised machine learning or a rules-based approach, can introduce complexity in understanding how an output was reached. Further, the scope for bias, unfairness, and discrimination from how systems are trained and deployed has raised concern (Benjamin, 2019). When used in policing, there is greater need for certainty in how decisions are made and explaining the rationale, given the UK model of policing by consent, which could be challenged by impacts of errors and inaccuracies. Thus, whilst AI can play a key rolein supporting human decision making in policing, there is greater need to question the societal, legal, and ethical implications of emerging uses. Current and emerging uses of AI in policing and biometric systems, like LFR, has prompted extensive regulatory and legal discussion (Information Commissioner's Office 2021; Oswald, 2022; Purshouse and Campbell 2022; Fussey and Murray; 2019; Urquhart and Miranda 2022), in addition to wider critical discussions of societal impacts of algorithmic systems like Emotional AI (McStay, 2018).

At the UK level, the UK Information Commissioner Office (ICO) has cautioned against widespread use of biometric systems, such as emotion recognition and LFR in a recent Foresight Report (Information Commissioner's Office 2022). There are also questions around scope of technology and legal oversight. For example, the Data Protection Act 2018 and Scottish Biometrics Commissioner Act 2020 both focus on the nature of biometric data as identifying an individual. Yet, some biometric AI systems, like emotion recognition, may not focus on identification. This can lead to challenges in establishing if such systems are legally in scope (McStay and Urquhart 2019; Ryder 2022). Further, regulatory oversight is shifting too e.g. UK Data Protection suggests shifting oversight of LFR to Investigatory Powers Commissioner's Office (IPCO), in an already existing patchwork of regulatory frameworks and oversight (Ryder, 2022). In England and Wales, there have been high profile uses of LFR by the Metropolitan Police Service and South Wales Police force. The Bridges v South Wales Police court cases focused on human rights, equalities law, and data protection issues in their use of the NeoFaceWatch system. Challenges included the lack of due diligence around ethnic and gender bias in training datasets, lack of quality guidance that responded to how face watchlists are created, and inaccuracies in data protection impact assessments (Urquhart and Miranda, 2022). As a result, College of Policing guidance emerged to provide help with these issues (CoP, 2021).

At European level, the proposed EU AI Act has prompted much discussion around law enforcement use of biometrics and AI. In the most recent Parliamentary version, in line with earlier calls from EU data protection bodies for bans, Emotion Recognition use by law enforcement has been called for to be banned by the EU Parliament, alongside police use of LFR in public spaces. Existing research has also shown that many police officers and other professionals involved in law enforcement activities remain sceptical about the role of LFR and other intelligent biometric technologies (Andalibi and Buss 2020; McGuire 2021; Urquhart and Miranda 2022).

Recently, Scotland has seen policy developments around AI and biometrics too. The landscape is shifting with the Scottish Government's AI Strategy, the ETIAG (Independent Advisory Group) review of police use of emergent technology, Justice Sub-Committee on Policing, and the establishment of the Scottish Biometrics Commissioner and their Code of Practice. The Code seeks to, among other things, promote and protect human rights, privacy, and public confidence in police acquisition, retention, use or destruction of biometric data. This is by adherence to 12 principles including necessity, proportionality, and lawfulness of deployments, alongside promoting equality, using privacy enhancing approaches, ensuring both public safety and public good, and protecting vulnerable groups. Further, the Commissioner has investigatory powers to monitor compliance with the Code providing real powers (Scottish Biometrics Commissioner, 2022).

Thus, there is much discussion around how best to regulate AI and biometric technologies. Our Design Fictions help to reflect on these issues by focusing on three examples set in Scotland, with police use of LFR, Emotion Recognition and DNA phenotyping. These scenarios develop from and build on existing uses of AI and biometric technologies in wider UK policing to consider future scenarios of use. This includes camera-based systems like LFR, Body Worn Video (BWV), and drones, through to thermal imaging and DNA profiling. Scotland (which currently does not use LFR, for example), has an opportunity to learn from and take a different direction from other jurisdictions in how biometric AI technologies are adopted in the future. Our work seeks to inform those discussions and critically reflect on emerging directions for biometric AI in law enforcement.

[1] Emotional AI Lab https://emotionalai.org

PART 2. INTRODUCING DESIGN FICTIONS

PART 2. INTRODUCING DESIGN FICTIONS

1. The Method

Briefly, Design Fiction is the development and presentation of diegetic prototypes (Bosch, 2012; Sterling, 2013) – designed objects or technologies that exist in a fictional world – using a narrative frame. Positioning the technology within a fictional world and exploring its effects through stories encourages a focus on people's lived experiences when interacting with technology. Design Fiction has been conceived as a creative technique but also a research method (Markussen & Knutz, 2013), as it aims to support consideration of potential futures by using prototypes and narratives that explore the consequences of new technology implementation. It also has the potential to afford movement towards preferred futures, by enhancing awareness of the ramifications of technological development and supporting the elaboration of guidance and regulation.

Some proponents of Design Fiction suggest the need for a physical instantiation of the diegetic prototype (Bleecker 2009), while others foreground the uses of narrative (Jensen & Vistesen, 2017). We position ourselves closer to the latter group, employing a narrative design fiction approach developed for a previous project on Emotional AI (Laffer 2022). For the roundtable, we explored three different technologies, positioning the diegetic prototype(s) along current development trajectories in Live Facial Recognition (LFR), Emotional AI, and DNA Phenotyping, creating three short multimodal stories (that combined text and images) of roughly 1000 words each.

Our approach to Design Fiction was originally developed to introduce emergent technology to citizens in focus groups (Laffer 2022; Urquhart, Miranda and Laffer, 2022). We believed it could fruitfully be used, when augmented with explicit discussion points, with expert stakeholders to afford meaningful discussion of concerns and impacts of new technology, particularly around governance. Due to the expertise of the audience, we decided to present the technology as near future, retaining plausibility but furthering the horizon of impacts that could be discussed.

To develop the design fictions, initially different points of tension and concern were discussed by the team, and incorporated into draft narratives, drawing on the team's past research, and expertise. These were initially text-only while undergoing revision and refinement, drawing on insights from the rapid literature review. When the text was finalised it was transferred to Twine, an interactive fiction writing tool, where multimodal components were added, ranging from location images and character portraits that supported the creation of the fictional world, to more specific diegetic objects (such as DNA phenotyping reports) that facilitated the introduction of the technology and explored specific concerns (for example, the impact of variation in image generation based on demographic characteristics). The full stories can be viewed here: https://biometricai.neocities.org/

2. Design Fiction Scenarios

We will present the Design Fiction 1. [Live Facial Recognition], and Summaries of Design Fictions 2 [Emotional AI] and 3 [DNA Phenotyping].
Design Fiction 1. Live Facial Recognition

Part 1.
Sam was a bit nervous. She thought it was important to join the March protesting the statues in George Square and hopefully draw people's attention to the country's colonial past. But now she was in the crowd, she was getting more concerned about rumours of a counter protest by groups like the Loyalist Defence League. She really didn't want to get caught up in any violence.

As the crowd advanced down North Hanover Street, she watched the drones slowly track them, their whine overhead cutting through the deeper human hubbub. The drones picked out congestion points where people bunched together. They hovered and dipped, like dragonflies momentarily alighting, to scan people's faces and make identification requests.

As Sam squeezed in among the protestors approaching the Square, she could see she was going to have to pass under a drone, the black eye of its camera monitoring the crowd below. Before the protest, her mother had insisted that she update her biometric passport on her phone. She had made Sam agree to share her details with anyone doing security checks to keep her safe and out of trouble. This was a drone though, not a security guard or police officer.

As the drone dipped towards her, Sam decided to follow her mother's advice. She got out her phone and opened her Biometric Passport app. The screen flashed:

Part 1

Sam was a bit nervous. She thought it was important to join the March protesting the statues in George Square and hopefully draw people's attention to the country's colonial past. But now she was in the crowd, she was getting more concerned about rumours of a counter protest by groups like the Loyalist Defenc League. She really didn't want to get caught up in any violence.

Sam taps 'AGREE'
Sam continued to read:

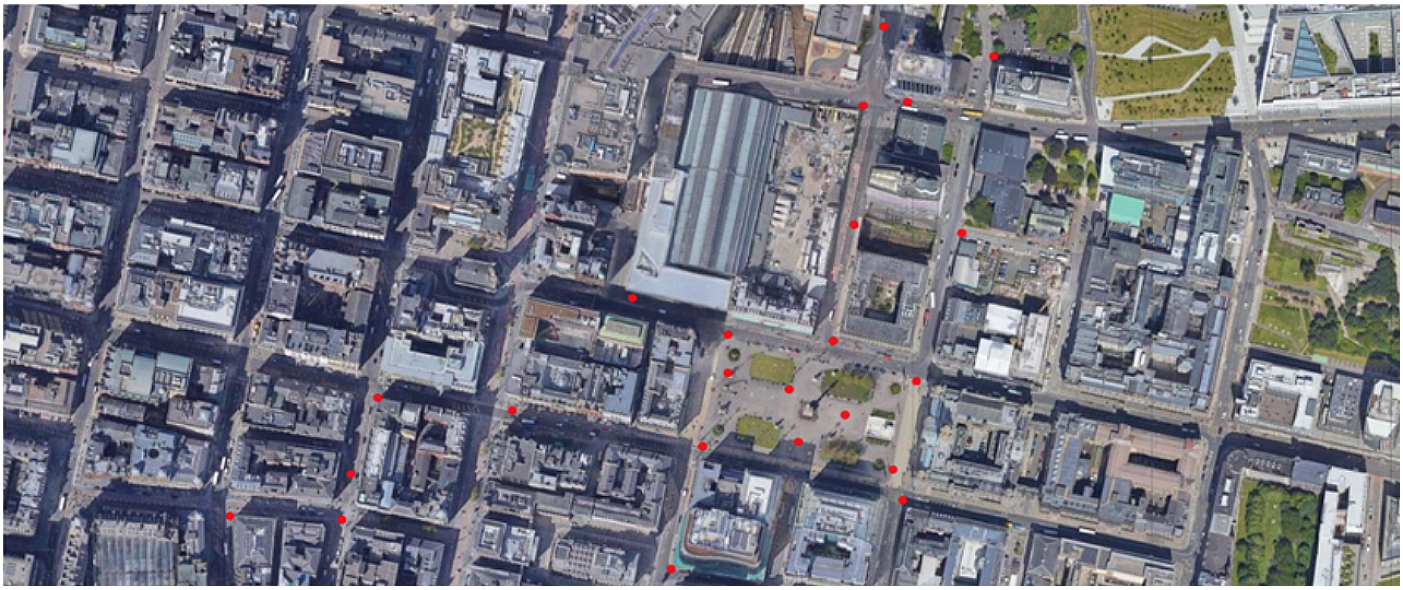
1. *Biometric Handshake Actions Required*
   Perform Face Scan
2. *Compare Stored Biometric Marker [Marker Random Select: id#IRIS]*
   Confirm?
   All data processed onboard Drone.
   Full Details Click Here

She looked up at the drone so it could get a good image of her face and eyes. Her phone beeped again.

Biometric Handshake Complete

1. *Facial Recognition Complete*
   Outcomes:
   Negative Match to suspect list
   Positive match to stored Biometrics
2. *Biometric Identity check (IRIS)*
   Outcomes:
   Negative Match to Suspect List
   Postiive Match to Stored Biometrics

Part 2



The technician monitored the drones' movement on the screen, flashing points on a map marking the edge of the crowd, slowly drifting to keep pace with the protest. These drones were relying on thermal sensors, finding the points where the heat of the crowd of people began to dissipate and then facing in with cameras turned towards the protestors.

Part 2.

The technician monitored the drones' movement on the screen, flashing points on a map marking the edge of the crowd, slowly drifting to keep pace with the protest. These drones were relying on

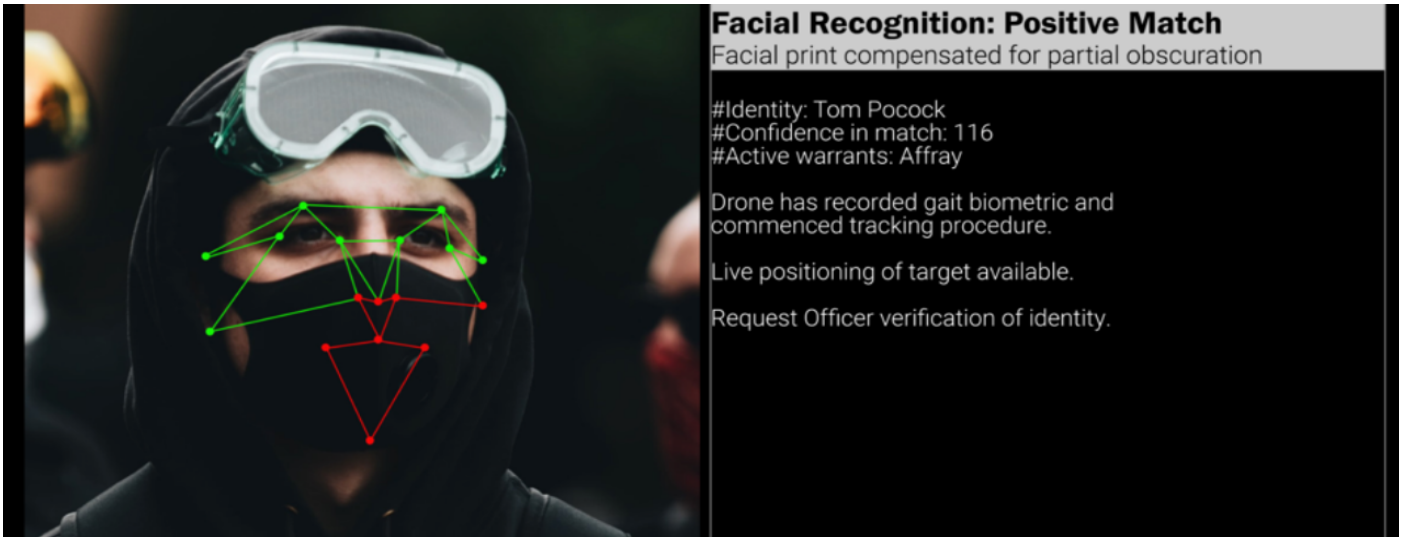
thermal sensors, finding the points where the heat of the crowd of people began to dissipate and then facing in with cameras turned towards the protestors.

The technician checked the live data feed being relayed and compared them to updates from the few officers on crowd control duty; the drones appeared to be operating effectively. The tech suspected the main protest would be relatively peaceful. The drones had yet to suggest any positive matches using facial recognition.

Of greater concern were the counter protestors, more loosely grouped and travelling faster. The drones were using multiple sensors to combine thermal data with individual gait and movement tracking. Using this information, they were able to identify potential flare points and monitor the people who moved into these areas.

Given the watchlist's focus on serious anti-social and violent behaviour, it seemed likely that they would find the people on the watchlist at these points; or at least those on the watchlist who might be about to commit further criminal acts.

"Targeted surveillance to find those most likely to re-offend", the tech thought. This is what the drones offered. The computer emits an alert. One of the drones has sent through a positive match.



P**art 3.**

Tom pulls the scarf further up his face. "Hands off our history!" he chants, joining in with the others as they march down the road. Tom hears a drone whir past overhead, swiftly overtaking them before keeping pace just ahead, its camera pointed in their direction. Someone in the group shouts 'Don't let it record you', followed by 'Scatter'. Tom doesn't wait, haring off down a side alley away from the protest.

He keeps running until he can't hear the drone's whine anymore. Out of breath, he stops at the corner of Bath Lane, and folds over with his hands on his knees. He hears heavy boots approaching and feels a sinking feeling in his stomach. He looks up at two police officers.

He recognises one of the officers, who says, 'Hello, Tom.'

The other officer points skywards, 'Our drone has given us a positive match using Facial Recognition and tracked you using biometric gait data. We will now carry out an ID check to confirm your identity'.

Tom swears under his breath.

Part 4.

After arresting Tom Pocock, the officers make their way back to the fringe of the protest. They are stopped on the way by a man accompanied by a child.

'What the hell is going on? That drone almost took my head off!'

The officers attempt to placate the man: 'We can assure you that the onboard camera and sensors would stop that happening.'

'Cameras? Are you taking pictures of us? You can't do that!'

'They are following the protest, sir.'

'And what if I wanted to join the protest? Seems like a good idea – but no way am I letting you record me and my child.'

'We're only checking faces against a watchlist, and that's only people who have engaged in or are suspected of prior criminal activity. Anything else is deleted from the drones before it's shared.'

'Oh yeah, right. And they actually do that? And what if your little spies in the sky spot me dropping litter or something? Are they going to take my picture and issue a fine?'

'As I said, we're only focussed on a specific watchlist.'

The man glares at them before picking up his child and storming off. The officers watch him go.

Design Fiction 1. In the first fiction discussion topics included: **Legalities under data protection law** in terms of lawfulness, fairness, accountability e.g., impact assessments; **Human Rights Implications** such as quality of law, proportionality, and necessity of measures; **Policing by consent** through technology and responding to citizen concerns; routes for **recourse for citizens** to question, or challenge use of technologies; implications of **integration of multiple technologies** (e.g., drones + LFR + BWV).

Design Fiction 2. Emotional AI

In this story a police officer is called to a domestic disturbance in a coastal town, where he is confronted with an argument between two migrant workers. A piece of body worn Emotional AI detects his rising stress level (based on heart rate) and advises him to pause and calm down. He uses this advice to regulate his initial response to the situation. The Emotional AI system then assists the officer by making predictions on the emotional stated of the workers, using video and audio data that it collects and analyses live.

In Fiction 2, discussion topics included: How automated reading of biometric traits **shapes police decision making; accuracy of systems** in practice e.g., contested models underpinning AI system and biases; **vulnerability of targets of biometric AI systems; Public Sector Equality duty** to engage with impacted communities and consider concerns and needs; capacity in policing to invest in resources vs utility e.g., more technology vs recruiting more officers.

Design Fiction 3: DNA Phenotyping

This story is set during a meeting between members of a police task force and scientists at a private lab where early trials of DNA phenotyping are being discussed. After a technician arguedd the technology, three different case studies are presented: 1) The search and rescue of a missing teenager in the Scottish Highlands, using DNA found on an item of clothing; 2) The creation of an aged-up portrait, using DNA phenotyping and AI-image generation, in order to produce new leads for a 30-year-old cold case; 3) The generation of suspect portrait based on DNA left at the scene of a violent crime. This image is subsequently run through facial recognition software to identify the suspect.

In Fiction 3 discussion topics included: What are the expectations and beliefs in **the science vs reality of errors/failure?; operational concerns** around use of novel tech in criminal investigation process and compromising evidence or prosecutions if it fails e.g. unfair trials; **Fragmented legal frameworks** and regulatory oversight; **transparency in procurement** of private sector technologies and standards of public scrutiny; **embedding biases** around protected characteristics such as race, gender, disabilities.

PART 3. SYSTEMATIC LITERATURE REVIEW

PART 3. SYSTEMATIC LITERATURE REVIEW

This report provides a descriptive overview of the social, ethical, and legal issues of Biometric AI use in Law enforcement. It focuses on relevant scholarly and policy research literature since 2018, as well as suggestions and recommendations offered by and outlined in the literature to help mitigate the existing challenges, tensions and limitations identified. The review findings were used to develop three design fiction scenarios to envision future uses of biometric AI technologies. This was with the aim of facilitating awareness and discussion amongst professionals working in law enforcement, policy and practice of the tensions and issues that may emerge from the use of these technologies in the future.

A key problem with emerging technologies is how the potential social, ethical, and legal issues can be dealt with before the technology becomes embedded in society (Brey 2017). According to Brey (2012) the foreseeable future in relation to technological development and embedding can be equated to a time frame of 10-15 years. This means that the 'emerging' phase within technological development may take up to 15 years and thus, it may take up to 15 years before the consequences associated with this form of technology may become fully known (Stahl et al., 2017, Brey 2012). Once a technology becomes entrenched within an institution, it can be more difficult to make changes (Brey 2017). Therefore, understanding the outcomes of existing research can help us anticipate the possible future consequences of its wider implementation within a specific sector (Whittlestone 2019). Further, the full impact and consequences associated with these technologies are uncertain and ambiguous (Sollie 2007).

The systematic review focused on a range of research questions:

1 **What is known** from the literature about the social, ethical, and legal implications of biometric AI adoption in law enforcement?
2. What possible **solutions or recommendations** have been made in the existing literature to help mitigate the social, ethical, and legal issues associated with biometric AI? Will they help to inform future decision-making and standards for best practice in the wider adoption and dissemination of these technologies in law enforcement?
3. What is the **nature of the existing research evidence base** exploring these issues (i.e., Qualitative interview evidence, trials of these technologies in policing contexts, analysis of existing literature etc)? This may be useful for identifying gaps in the existing knowledge base and areas where future research may be required.

Each of these questions will be answered for each of the three specific types of biometric AI technologies in question: 1) LFR, 2) intelligent behaviour and emotion recognition, and 3) DNA (predictive) phenotyping. The rapid review methodology consisted of two components:

1. <u>Systematic search and review of the published academic research literature</u>

- This focuses on the development, trial, implementation, use and dissemination of Biometric AI technologies in law enforcement.

- This combined systematic and narrative techniques to review the existing academic literature, adhering to key principles of systemic reviewing (Bryman 2012) and allowing subjective evaluation of the literature to determine relevance (Snilsveit et al., 2012).

- Web of Science, Scopus, and JSTOR were consulted using combinations of the following keywords:

Each of: Law Enforcement; Policing.

Together with each one of: *Biometric(s); Artificial Intelligence; AI; Artificial Intelligence Technology(ies); Smart Technology(ies); Biometric AI; Biometric Identification; Predictive Technology(ies); Live Recognition Technology(ies); Intelligent Biometric Identification; Live Facial Recognition Technology(ies); Intelligent Face/facial Recognition; Emotion Recognition Technology(ies); Emotion Detection Technology(ies); Behavio(u)r Recognition Technology(ies); Intelligent Behavio(ur) Recognition; Predictive Technology(ies); Smart Recognition Technology(ies); DNA Phenotyping Technology(ies); Predictive Phenotyping; Intelligent Phenotyping; FDP.*

AND at least one or more of: *Social, Ethic(al or s), Legal; Law, Challenge(s) Issue(s), Implication(s), Risk(s), Barrier(s), Criticism, Strength, Limitation, Society; Decision Making; Best Practice: Evidence; Evidence Based; Recommendations; Policy: Practice; Legislation; Regulation; Standard; Standardisation: Development; Implementation; Use.*

- This generated a total of **227** initial documents. After removing articles older than 5 years (pre-2018) to capture recent developments, those in another language (due to resource issues of translation) and duplicates, this went to **117** documents. Titles and abstracts were then evaluated to sort for relevance to research questions and project objectives. This then left us with **62** documents.

- Analysis and coding of the sixty-two documents in the sample obtained via the systematic search process was undertaken using qualitative descriptive analysis of the contents of each document to identify and code for key themes inductively (Sandelowski 2000). This process enabled the social, ethical, and legal issues associated with the different technologies to be identified, along with suggestions and recommendations for mitigating challenges or problematic issues identified, and the nature of the evidence base of the research for each type of biometric AI technology.

2. Review of the policy-relevant (grey) research literature

- Sourcing and reviewing relevant academic research reports, practice-based evidence reports, Government reports, and policy-relevant research reports, which were not available via the academic research literature databases.

- An abridged version of the Delphi Technique was used to source reports, through consultation with senior members of the project with high levels of expertise and experience in this area of research. The Delphi Method involves drawing on the extensive knowledge, skills, and expertise of academic experts and/or practitioners working in the issue of relevance (Barrett and Heale 2020).

- These were coded and analysed in the same way as the literature. An additional 15 documents were included this way, giving an overall total of **77** documents analysed.

SECTION 1. FACIAL RECOGNITION IN LAW ENFORCEMENT

SECTION 1. FACIAL RECOGNITION IN LAW ENFORCEMENT

Introduction

Facial recognition technologies aim to identify individuals based on their distinguishing facial features (Davis and Harriss, 2018). Biometric facial attributes are inherently linked to a person and facial recognition technologies are used in two main ways: 1) verification for ensuring someone is who they say they are by comparing a biometric attribute to a previously obtained 'reference' record, such as checking an individual's face matches their passport photo, and 2) identification for determining who a person is by comparing one or more biometric attributes against a set of reference records collected from multiple people (ibid). Facial recognition technologies have the potential for providing new tools to aid law enforcement, however there is considerable debate over their efficiency, accuracy, and legitimacy and as to whether the regulation of biometric technologies is adequate for police.

The uses of live facial recognition (LFR) technologies differ to other forms of facial recognition techniques. LFR technologies are typically deployed in a similar way to traditional Closed Circuit Television Surveillance Systems (CCTV). The technology is directed towards everyone in a particular area rather than a specific individual. Therefore it can capture all those individuals passing within a certain range of the camera automatically and indiscriminately. Biometric data is therefore collected in real-time and potentially on a mass scale. There is often a lack of awareness, choice, or control for the individual in this process (Information Commissioner's Opinion 2021). These technologies involve a process of data capture, whereby a sensor captures the biometric characteristics of the user, followed by feature extraction where the data captured by the sensor are processed into digital form containing only the key distinguishing features required to identify the person. The template is then stored for future comparison as a reference record, either on a central database or on local storage systems. Algorithms compare the biometric data input with the reference records and provide a score for how close the match is. Depending on whether the score is over a certain threshold, the system declares it a match or non-match (Davis and Harriss, 2018). Most of these technologies are therefore probabilistic and involve some degree of error, but a higher threshold will produce fewer false matches but also more false non-matches and vice versa (ibid).

3.2.1: Social and ethical issues

Thirty-two of the fifty-one documents focusing on LFR technologies identified a variety of social and ethical issues associated with the implementation and use of these forms of technology in law enforcement.

Trust was a major ethical issue identified in acceptance of the use of these technologies and was mentioned in twelve of the documents (Ada Lovelace Institute 2019; Bradford et al 2020; Fontes and Perrone 2021; Davis and Harriss, 2018; Guo and Kennedy 2022; Kosta et al 2023; Hill et al 2022; Information Commissioner's Office 2021; Urquhart and Miranda 2022; McGuire 2021; Williams 2020; Connon et al 2023). Two of these explained that an important key issue or challenge to the trust or acceptance of these technologies was a mismatch between public awareness of the technologies and specific knowledge about these technologies (Ada Lovelace Institute 2019; Guo and Kennedy 2022). Kosta et al (2023) found that in Germany, the UK, the US and China, people were more likely to trust the use of live facial recognition technologies by the

police in public spaces if they trusted government officials and institutions. Similarly, Bradford et al., (2020) explored the results from a London-based study analysing public responses to LFR technologies which enable police to conduct real-time automated identity checks in public spaces. They arguedd that public trust and legitimacy are important factors in the acceptance and rejection of these technologies. McGuire (2021) explained that perceptions of the potential misuse of these technologies and concern about the denial of rights can threaten the viability of policing and lead to questions about the limits of automation in policing. Connon et al (2023) discussed how the public is often sceptical about how the police will use this technology and for what particular purposes and argued that if police use of LFR is perceived as illegitimate, police-citizen relationships may deteriorate, especially for marginalised communities.

The second key issue identified was that of **consent**, which was mentioned in six of the documents (Ada Lovelace Institute 2019; Connon et al 2023; Dechesnea and Dignum 2019; Fontes and Perrone 2021; Fontes et al 2022; Guo and Kennedy 2022). The Ada Lovelace Institute report (2019) explained that over 50% of people in the UK want the option to be able to opt out or to be asked to consent to the use of this technology. The potential covert use of this form of technology could also potentially deprive individuals of their agency when it comes to privacy and protection of their personal data (ibid).

The third issue mentioned in six of the documents concerned **the fear of the normalisation of surveillance in society** (Ada Lovelace Institute 2019; Douglas and Welsh 2022; Fontes and Perrone 2021; Fontes et al 2022; Smith and Miller 2022). For example, the Ada Lovelace Institute report (2019) explained that the majority of respondents from a UK survey of attitudes towards LFR were concerned that these technologies were part of an expanding 'surveillance creep'. However, the report also noted that the majority support these technologies when there is a clear public benefit to the use of the technology and when appropriate safeguards are put in place. In addition, LFR technologies risk greater exposure of the population to the increased risk of stated-citizen power imbalances based on increased access to biometric information and individuals' lives and activities (Fontes et al 2022).

The fourth issue identified was a concern about the **lack of safeguards** concerning the use of these technologies or clarity in the safeguarding of data that these technologies involve, such as via the development of shared ethical frameworks and regulations (Ada Lovelace Institute 2019; Babuta and Oswald 2020; Connon et al 2023; Dechesnea and Dignum 2019; Dworzecki and Nowicka 2021; Davis and Harriss, 2018; Guo and Kennedy 2022; Leslie 2020; Sarabdeen 2022). This was discussed in nine of the documents. The Ada Lovelace Institute (2019) report explained that support for these technologies remains conditional upon there being appropriate limitations and safeguards as to their use. The lack of ethical standardisation concerning their implementation and use was also deemed to be particularly problematic (Deschesnea and Dignum 2019). Lack of coherent regulations and standards can also limit the acceptability of these technologies amongst law enforcement officers (Dworzecki and Nowicka 2021). In Poland, police officers' acceptance of these technologies was affected by a lack of coherent regulation surrounding their use, a lack of standardised rules concerning access by all parties, and a lack of knowledge in the organisation about the potential benefits and risks associated with these technologies (ibid). The Ada Lovelace Institute (2019) report also explained that people expect the government to place limits on the use of these technologies and expect these to be detailed in policy and complied with.

Another issue of public concern was that of **third-party access to the data**, including by organisations working in partnership with the police, which was mentioned in eight of the documents (Ada Lovelace Institute 2019; Deschesne and Dignum 2019; Dworzecki and Nowicka 2021; Fontes and Perrone 2022; Information Commissioner's Office 2021; Sarabdeen 2022; Smith and Miller 2022). Members of the public have even lower levels of trust in private sector partners over concerns

about whether their data will be used ethically (Ada Lovelace Institute 2019). Biometric data was noted to be especially sensitive, meaning that concerns about third-party access and the potential for misuse was more concerning than for other forms of personal data (Information Commissioner's Office 2021).

The **risk of bias and discrimination**, including racial and ethnic bias, embedded within these technologies was another ethical issue raised in relation to this technology. This was discussed in 18 of the documents (Ada Lovelace Institute 2019; Alikhademi et al 2022; Colman 2021; Chowdhury 2019; Connon et al 2023; Hood 2020; Deschesnea and Dignum 2019; Didhwala 2020; Davis and Harriss, 2018; Kosta et al 2023; Leslie 2020; Nkande 2020; Urquhart and Miranda 2022; Williams 2020; Noriega 2020; Asaro 2019; McKendrick 2019; Whittelstone 2019). For example, Hood (2020) explored the integration of facial recognition into police body-worn camera devices and discussedthe political dangers of these technologies. Hood (2020) arguedd that these technologies risk reinforcing normative understandings of the body and explored how facial recognition surveillance devices pose enhanced risks for marginalized groups. Hood (2020) explained that body worn cameras with facial recognition devices present a number of socio-political dangers that reinforce the privilege of perspective granted to police in visual understandings of law enforcement activity and risk reinforcing racial marginalization. Similarly, Chowdhury (2020) argueds that live facial recognition represent a form of monitoring technology which has a long history of being deployed primarily against ethnic minorities. Chowdhury (2020) also explained that ethnic minorities are substantially at risk of being over-policed and discussed how improvements in accurate facial recognition technologies will likely still exacerbate racial inequalities, because it is highly likely that the technology will be disproportionately used against those communities. This author uses the example of the London trials of this technology by the Metropolitan Police at the Notting Hill Carnival to highlight the inequalities of outcomes and to show the dangers resulting from failure to carry out an equality impact assessment before deploying this form of technology. The Ada Lovelace Institute (2019) report explained that facial recognition technologies are worse at identifying faces of ethnic minorities. In addition, the processes and datasets that support the development of these technologies are not equally representative or responsive to social diversity (ibid). As a result, their use risks embedding problematic bias, resulting in greater inaccuracies in identification for some people compared to others. Didhwala (2020) explained that in the UK, data captured using live facial recognition technologies is not retained unless there is a match. However, inaccuracies in matching can result in a disproportionate amount of data being retained for certain groups, often the most socially marginalised people (ibid). Nkande (2020) argueds that facial recognition results in 'automated anti-Blackness' owing to data driven decision-making processes which are assumed to be objective despite algorithms 'seeing' the world through the eyes of their creators, containing an inbuilt bias against racial minorities. In addition, the unequal use of these technologies against African American communities can also be arguedd to perpetuate historical patterns of racism through enhanced surveillance (ibid; Alikhademi et al 2022). Noriega (2020) also discussed how both racial and gender bias may be embedded in the design of facial recognition technologies.

One article within the sample identified another potential problem particular to the use of facial recognition (Urquhart and Miranda 2022). They arguedd that one of the social risks associated with this form of technology is that they risk the **biodeterministic framing of criminality** based on facial data, which can erode the presumption of innocence and lead to the increased surveillance of certain groups of people and individuals in possession of certain facial characteristics.

Another important social and ethical issue identified was that of **privacy** with one concern being that these technologies can be deployed semi-covertly. This was mentioned in eighteen of the documents. The semi-covert deployment of these technologies results in a blurring of the boundary between the private and public space and means it is not always clear when it is being used or by whom it is being deployed (Ada Lovelace Institute 2019; Almeida et al 2022; Bragias et al 2021;

Connon et al 2023; Deschesnea and Dignum 2019; Douglas and Welsh 2022; Didhwala 2020; Eneman et al 2022; Keenan 2021; Fontes et al 2022; Davis and Harriss 2018; Guo and Kennedy 2022; Kosta et al 2023; Sarabdeen 2022; Smith and Miller 2022; Urquhart and Miranda 2022; Chowdhury 2020; Fussey and Murray 2019). For example, Keenan (2021) explored how in the case of R (on the application of Bridges) v Chief Constable of South Wales Police, the Court of Appeal held that the deployment of live facial recognition technology by the South Wales Police Force (SWP) was unlawful because it violated the right to respect for private life under Article 8 of the European Convention on Human Rights, lacking a suitable basis in law. They also explored how the Data Protection Impact Assessment conducted under section 64 of the Data Protection Act 2018 failed to assess the risks to the rights and freedoms of individuals processed by the system. Similarly, Smith and Miller (2022) explain that facial recognition technologies which involve the automated comparison of facial features cedarry significant privacy implications that require law and regulation.

Questions also arose about the **legitimacy of the use of these technologies** (Bradford et al 2020; Bragias et al 2021; Connon et al 2023; Dechesnea and Dignum 2019; Didhwala 2020; Dworzechi and Norwicka 2021; Eneman et al 2022; Fontes and Perrone 2021; Davis and Harriss 2018; Hill et al 2022; Smith and Miller 2022; Beck 2021; Hobson et al 2020; Asaro 2019), with the issue of legitimacy being discussed in 14 of the documents reviewed. For example, Beck (2021) discussed the issues of fairness and legitimacy in relation to the use of AI in law enforcement, predictive policing and risk assessment and explained that concerns about fairness are rooted upon concerns about the prospects of bias and an apparent lack of operational transparency. Beck also showed how media coverage of the use of AI can exacerbate these concerns (ibid). Hobson et al., (2021) focused on the issue of legitimacy in relation to algorithmic policing and shows that members of the public tend to view a decision as less fair and appropriate when made by an algorithm, compared to decisions made by police officers. This also shows how perceptions of fairness and appropriateness were strong predictors of support for police algorithms. They conclude that algorithm decision making may damage trust in the police, particularly in cases when the police rely heavily or solely on algorithmic decision making. Similarly, Asaro (2019) discussed the risks around the use of data-driven algorithms in policing and how this raises questions about fairness by effectively treating people as guilty of (future) crimes for acts they have not yet committed and may never commit, and how the use of predictive information systems may shape the decisions and behaviours of police officers. In addition, perceived illegitimate uses of the technologies risk threatening police-citizen relationships or intensify pre-existing issues (Bragias et al 2021). However, perceived legitimate use of these technologies can help to alleviate privacy concerns around the deployment of these technologies (ibid). Legitimacy is contingent upon perceived risk to security, however the extent to which these technologies can limit the actual threats to security depends on multiple factors, including the amount of data captured and who is already on a watchlist (Didhwala 2020). However, as Dworzecki and Norwicka (2021) explain, when used well, these technologies can help to enable the detection of crime and its perpetrators. But if used negligently or inappropriately, they can violate an individual's rights and freedoms leading to a loss of perceived legitimacy (ibid). In addition, Eneman et al.'s (2022) study of the use of Clearview AI live facial recognition technologies in Sweden showed that threats to the privacy of the biometric data and the algorithms using them has the potential to lower public perceptions of the legitimacy of these technologies. As Fontes and Perrone (2022) noted, the benefits of deploying these technologies must outweigh the risks and be perceived to do so for their use to be considered legitimate.

Security was another important concern as the data gathered from deploying facial recognition technologies can reveal a range of intimate information about an individual and the context in which they live (Ada Lovelace Institute 2019; Bragias et al 2019; Connon et al 2023; Eneman et al 2022; Davis and Harriss 2018; Sarabdeen 2022; Hayward and Maas 2021). This was explored in seven documents. The consequences of the misuse, abuse, loss, or theft of the data are also

graver than for other types of personal data because biometric information such as one's face cannot be readily changed like a person's bank details can in the event of a breach (Ada Lovelace Institute 2019). One article explored the potential risk of the application of AI, including live facial recognition, by perpetrators of crime (Hayward and Maas 2021).

The **accuracy** of these technologies was also another important ethical consideration, and which was discussed in eleven documents (Becerra-Riera et al 2019; Colman 2021; Didhwala 2020; Connon et al 2023; Alikhademi et al., 2022, Whittelstone 2019; Beck 2021; Hobson et al., 2020; Asaro 2019; Wright 2021; McKendrick 2019). In real world situations, live facial recognition technologies can be far less accurate than in laboratory conditions owing to varying lighting contexts and occulusions, as well as due to moment-to-moment changes in facial expressions which they can struggle to read accurately (ibid). Becerra-Riera et al (2019) also note that characteristics known as 'soft biometrics' such as face shapes, gender, age, and skin can be especially difficult for the technologies to identify in real-world conditions. They explain that age is the hardest to estimate owing to variation in how an individual's facial features may age as a result of internal and external factors. Skin tone and gender can also be inaccurately identified in live situations too (ibid). Another issue is that problems of accuracy tend to be understood by law enforcement officers as failures in the performance of these technologies rather than as signs of human and algorithmic biases (Colman 2021). This can further amplify existing inequalities in identification accuracy and exacerbate or create tensions between police and members of the public (ibid).

Possible solutions

Fourteen of the documents that discuss the social and ethical challenges surrounding the use of live facial recognition technologies offer possible solutions to the identified challenges and limitations. Eight documents suggest possible ways to improve public trust in these technologies (Asaro 2019, Ernst et al., 2021; Whittlestone 2019; Bragias et al 2021; Hill et al 2022; Urquhart and Miranda 2022; Oswald 2019; Connon et al 2023). For example, Bragias et al (2021) explore how public trust in these technologies may be improved via increased transparency over their practices and greater communication to educate people about what the technologies entail and how their data will be collected, stored, and used. Hill et al (2022) argued that public trust could be improved through greater public engagement in police decisions regarding the acquisition, use and assessment of the effectiveness of live facial recognition technologies and the inclusion of citizen stakeholders in the development of ethical guidelines and oversight frameworks. Urquhart and Miranda (2022) argued that by adopting a pre-emptive approach to harm minimisation prior to the use of these technologies in practice may help improve public trust in the use of these technologies. Standards should also be required for experimental use of these technologies before they are deployed in practice (ibid).

Two documents offer suggestions about how to overcome the problems associated with a lack of standardisation in the ethical use of these technologies (Deschesnea and Dignum 2019; Didhwala 2020). Dechesnea and Dignum (2019) explore how concerns over a lack of standardisation for access and use may be alleviated through the design and implementation of a shared internal ethical standards framework, while Didhwala (2020) argued that greater standardisation will help to improve consistency and clarity concerning the storage of data.

Three documents discuss possible ways to improve the perceived legitimacy of the use of these technologies (Fontes and Perrone 2021; Guo and Kennedy; Urquhart and Miranda 2022). Perceived legitimacy of the use of these technologies may be improved by the use of assessments to be carried out in advance of the implementation of these technologies to identify the potential social and individual risks (Fontes and Perrone 2021) and by the implementation of a regulatory oversight framework or code of conduct to enforce the protection of human rights (Guo and Kennedy 2022).

In addition, the use of less intrusive technologies where they serve the same outcome should also help to improve the perceived legitimacy over the use of these technologies (Urquhart and Miranda 2022).

Concerns about third-party access and data sharing may be alleviated through clarity about how and by whom personal data will be accessed and/or shared (Fontes and Perrone 2021).

Two documents offer possible suggestions for reducing the bias built into these forms of technology as well as in their deployment (Nkande 2020; Urquhart and Miranda 2022). Nkande (2020) arguedd that the discrimination and bias against racial minorities associated with this technology may be reduced by centering minority groups in the design process. The involvement of marginalised groups in assessments of and in the development of policy interventions to address the unequal impacts of these technologies may also help to reduce bias and discrimination (Nkande 2020; Urquhart and Miranda 2022).

Connon et al (2023) argueds for a combined approach to mitigating the social and ethical challenges associated with this form of technology, seeking improvements in research, policy, and practice. They argued for the development of a set of shared concepts and terminology to develop an ethics of algorithms and the building of a more rigorous evidence base for the discussion of social and ethical issues surrounding the use of AI in policing. In addition, clear guidelines for the scrutiny and regulation of live facial recognition should be produced as part of a new draft code of practice which should specify the responsibilities for policing bodies regarding scrutiny, regulation, and enforcement of these new standards (ibid). Mandatory equality impact assessments for the collection and reporting of ethnicity data, along with a new national ethical approach based on Oswald's (2019) three-pillar approach that includes clear scientific standards for these forms of technology should also be introduced (ibid). Establishment of a national technology clearinghouse for ensuring robust scientific standards for AI technologies, as well as an algorithmic impact assessment policy should also help to alleviate concerns about the accuracy of these technologies. Furthermore, the adoption of an Ethics of Care approach (based on the work of Asaro (2019) to minimise the risk of harm in the dissemination and use of these technologies should also help to improve perceptions of fairness regarding these technologies (ibid). Law enforcement staff should also be trained in how to engage critically with the adoption and use of new technologies so that they are in a position to meaningfully engage in impact assessments (ibid). However, none of the documents reviewed offer any clear suggestions for improving limitations and challenges related to the issues of consent, privacy, increased surveillance, and security associated with this form of technology.

Evidence base

Of the thirty-two documents that discuss the social and ethical issues associated with LFR and their possible solutions, seventeen were based on review and analysis of the existing scholarly literature to draw conclusions and identify the potential issues. Nine were based on primary data from case studies involving the trialling and use of these technologies by police professionals in the UK, Canada, Sweden, and Poland. Three were based on survey data, one was based on interview data, and two were primarily based on case law analysis.

3.2.2: Legal issues

Eleven of the fifty-one documents focusing on LFR discussed the legal issues associated with this form of technology (Ada Lovelace Institute 2019; Almeida et al 2022; Connon et al 2023; Dudhwala 2020; Feraldo-Cabana 2023; Information Commissioner's Office 2021; Keenan 2021; Ryder 2022, Rapaso 2022; Purshouse and Campbell 2022; and Urquhart and Miranda 2022). The main legal issues identified with this form of technology relate to the safeguarding of Human Rights and equality, data protection, the law of evidence and the disclosure of evidence.

All eleven of the documents discussed the issue of the legal safeguarding of Human Rights and equality (Ada Lovelace Institute 2019; Almeida et al 2022; Connon et al 2023; Dudhwala 2020; Faraldo-Cabana 2023; Davis and Harriss 2018; Keenan 2021; Information Commissioner's Office 2021; Purshouse and Campbell 2022; Rapaso 2022; and Urquhart and Miranda 2022). Guest (2018) explained that live facial recognition use is regulated by the Human Rights Act of 1998, which stated that everyone has the right to respect for their private life. Urquhart and Miranda (2022) stated that more discussion is required as to the quality of current law to protect citizens from harm, as required by Human Rights law. Feraldo-Cabana (2023) argued that live facial recognition technologies pose a significant threat to Human Rights, including human dignity, the right to private life, the protection of personal data, non-discrimination, the rights of the child and the elderly, the rights of people with a disability, and the right to an effective remedy and to a fair trial. They argued that protection of these Human Rights is threatened by the fragmented nature of the legal landscape concerning the use of these technologies (ibid). Almeida et al (2022) also note that there is no standardised Human Rights framework and regulatory requirements that can be easily applied to facial recognition technology rollout. Purshouse and Campbell (2022) explain that, until recently, the use of facial recognition continued largely unabated by law because the Government and domestic courts were satisfied that police use of this form of technology is adequately reflected by existing statutory processes regulating the processing of this form of biometric data. However, they also explore how this was brought into question in England and Wales with the R (Bridges) v. Chief Constable of South Wales Police and Others (2020) EWCA civ 1050 case (ibid). Keenan (2021) explored tensions around interferences from facial recognition in the case too, particularly around tensions between interference with privacy at group and individual levels, and how this impacts assessments of necessity under Article 8(2).

Eight of the documents discuss the legal issues associated with this form of technology concerning data protection (Almeida et al 2022; Connon et al 2023; Faraldo-Cabana 2023; Information Commission's Office 2021; Davis and Harriss 2018; Keenan 2021; Raposo 2022; Urquhart and Miranda (2022). Raposo (2022) and Faraldo-Cabana (2023) discuss weaknesses within the EU General Data Protection Regulation in relation to live facial recognition technologies. For example, Faraldo-Cabana (2023) explore the different regimes around biometric data, for example stricter grounds for processing under GDPR, and Law Enforcement Directive safeguards around automated data processing. They argued fragmentation in the legal landscape can lead to a lack of clarity (ibid). Guest (2018) stated controllers seeking to deploy live facial recognition technologies must comply with all relevant parts of the UK GDPR and DPA 2018, including the data protection principles set out in UK GDPR Article 5, including lawfulness, fairness, transparency, purpose limitation, data minimisation, storage limitation, accuracy, security, and accountability. The Information Commissioner's Opinion (2021) report identified a broader range of potential data protection issues that can arise when live facial recognition technologies are used for the automatic collection of biometric data in public places, drawing on primary research involving reviewing data protection impact assessments. The key legal protection challenges identified were the automatic collection of biometric data at speed and scale without justification as to the necessity and proportionality of data processing, the lack of choice for individuals, the governance of watchlists and escalation processes, and the processing of children and

vulnerable adults' data (Information Commissioner's Opinion 2021). Another important issue that may be relevant to data protection analysis is where bias in facial algorithms could lead to unfair treatment of individuals (ibid). The report also stated that while all relevant elements of the legislation apply, problems can occur when the central legal principles of lawfulness, fairness, and transparency, including a robust evaluation of necessity, and proportionality, are not thoroughly considered before live facial recognition technologies are deployed (ibid). The report arguedd that considering these legal principles in advance is fundamentally important because live facial recognition technologies involve the automatic collection of biometric data, including on a mass scale, without individuals' choice or control. For their use to be lawful, controllers must identify a lawful basis and condition to process special category data and criminal offence data and must ensure that their processing is necessary and proportionate to their objectives. Controllers are accountable for their compliance with the law and must demonstrate that their processing meets its requirements. Before deciding to use LFR in public places, they should complete a DPIA. As part of this process, they must assess the risks and potential impacts on the interests, rights, and freedoms of individuals. This includes any direct or indirect impact on their data protection rights. The law also requires them to demonstrate that their processing can be justified as fair, necessary, and proportionate. Taken together, these requirements mean that where live facial recognition technologies are used for the automatic, indiscriminate collection of biometric data in public places, there is a high bar for its use to be lawful (ibid).

In terms of other legal frameworks, Urquhart and Miranda (2022) analyse recent UK case law on LFR use by police and show how it raises concerns surrounding data protection. They also explore how the proposed EU AI Act will shape future uses of this form of technology in policing at European level as technologies could be prohibited form of AI and never make it to market in the first place, or be classed as high risk and need to comply with new rules and design requirements (ibid). Relevant law enforcement legislation includes the Police and Criminal Evidence Act 1984 (PACE), in England and Wales, which allows police to take and retain fingerprints, DNA and facial images following arrest, for the purpose of solving or preventing crime. Also, in England and Wales, the Protection of Freedoms Act 2012 which amended PACE in response to a ruling from the European Court of Human Rights that the indefinite retention biometric data from people not convicted of a crime was unlawful. However, there are exceptions, as biometric charged with a serious offence may be kept for three years, while data from those data from those convicted of a recordable offence may be retained indefinitely. This Act also created the roles of the Surveillance Camera Commissioner, who encourages compliance with the Surveillance Camera Code of Practice, and the Biometrics Commissioner to oversee biometric information databases. In LFR trials, the Government said the database constituted a bespoke 'watch list' that may include people banned from attending certain events and people wanted in connection with a crime (ibid). However, questions have been raised about the adequacy of current legislation and regulation relating to the retention of custody images and to automated facial recognition technologies. The Camera Code of Practice stated that police use of facial recognition needs to be justified and proportionate, however the Surveillance Camera Commissioner has no power to enforce this. Connon et al (2023) argued that the use of this form of technology is highly likely to challenge the boundaries of the Criminal Procedure (Sc) Act 1995, Regulation of Investigatory Powers (Scotland) Act 2000, Investigatory Powers Act 2016, as well as compliance with the National Assessment Framework for Biometric Data Outcomes and prospectively the Scottish Biometric Commissioners' Code of Conduct (2022).

Possible solutions

Four documents also provide suggestions and recommendations for improving legal clarity over the use of these technologies and for mitigating some of the legal challenges surrounding data protection and the protection of Human Rights and equality (Almeida et al 2022; Raposo 2022; Ryder 2022; Connon et al 2023). For example, Almeida et al (2022) set out ten critical questions that need to be answered by lawmakers, policy makers, designers, and users of these technologies to provide clarity over the limits of their use. These are: 1) Who should control the development, purchase, and testing of facial recognition systems ensuring the proper management and processes to challenge bias? 2) For what purposes and in what contexts is it acceptable to use these tools to capture individuals' images? 3) What specific consents, notices and checks and balances should be in place for fairness and transparency for these purposes? 4) On what basis should facial data banks be built and used in relation to which purposes? 5) What specific consents, notices and checks and balances should be in place for fairness and transparency for data bank accrual and use and what should not be allowable in terms of data scraping? 6) What are the limitations of facial recognition performance capabilities for different purposes taking into consideration the design context? 7) What accountability should be in place for different usages? 8) How can this accountability be explicitly exercised, explained, and audited for, for a range of stakeholder needs? 9) How are complaint and challenge processes enabled and afforded to all? and 10) Can counter-AI initiatives be conducted to challenge and test law enforcement and audit systems?

Raposo (2022) advocates for the creation of a specific new law on the use of live facial recognition in law enforcement based on addressing existing data protection limitations within current EU law. Ryder (2022) provides ten recommendations for improving the current legislative framework concerning the use of this form of technology. These recommendations are: 1) For the provision of a new technologically neutral, statutory framework. Legislation should clearly set out the process that must be followed and considerations that must be taken into account by all public and private bodies before biometric technology can be deployed against members of the public. 2) For the scope of legislation to extend specifically to the use of biometrics for unique identification of individuals and for classification. This is because the legal framework needs to provide appropriate safeguards because of the rights-intrusive capacity of biometric systems. 3) For the statutory framework to require sector and technology specific codes of practice to be published which set out specific and detailed duties that arise in particular types of cases. 4) For a legally binding code of practice governing the use of live facial recognition technologies to be published as soon as possible, including public-private data sharing in the deployment of facial recognition products. 5) For the use of live facial recognition technologies in public spaces to be suspended until the new legislation and code of practice are in place. 6) For the code of practice and new legislation to supplement rather than replace existing duties arising under the Human Rights Act 1998, the Equality Act of 2010, and the Data Protection Act of 2018. 7) For a national Biometrics Ethics Board to be established and which should have a statutory advisory role in respect of public-sector biometrics use. 8) For the Biometric Ethics Board's advice to be published and summaries to be published by the deploying public authority in cases where these technologies are deployed contrary to the advice of the Ethics Board, explaining their reasons for rejecting the Board's advice, or the steps they have taken to respond to the Board's advice. 9) For the consolidation and clarification of the regulation and oversight of biometrics to address existing limitations resulting from the overlapping and fragmented nature of oversight. 10) For the legislation to also regulate private-sector use of these technologies and biometrics (at least to some extent) to address issues arising from the porous relationship between private-sector organisations gathering and processing biometric data and developing biometric tools, and public authorities accessing those datasets and deploying those tools.

Connon et al (2023) also make several suggestions for mitigating some of the existing legal challenges. They argued that at the outset of designing, adapting, or adopting an emerging technology, consideration should be given to how that technology is to be used to ensure compliance with the law of evidence. In addition, the relationship between those involved in the development and implementation of emerging technologies should be mapped for data protection purposes. Furthermore, research should be undertaken to consider the legal and ethical implications for the use of emerging technologies in policing activities involving children, with a view to ensuring compliance with the United Nations Convention on the Rights of the Child. An equality and human rights impact assessment should form a compulsory part of the trial and adoption of any new technology policy. This should facilitate consideration of these issues on a cyclical process before adoption, during deployment, and after deployment. These impact assessments need to go beyond the minimum legal requirement of data protection and should consider the full range of impacts and consequences, including social and ethical impacts (ibid). Training should be given to all officers involved in the use or monitoring of emerging technologies to ensure they are aware of their equality and human rights obligations in the context of its use, and data on the equality impacts of trial use of technologies should also be made publicly available (ibid).

Evidence base

Of the eleven documents that discussed the legal issues associated with LFR, six were based on a review of existing legal cases (Almeida et al 2022; Feraldo-Cabana 2023; Keenan 2021; Ryder 2022; Raposo 2022; Purhouse and Campbell 2022). One was based on a combination of interviews with frontline law enforcement officers and the existing case law (Urquhart and Miranda 2022), and another was based on survey data (Ada Lovelace Institute 2019). Three were based on a review of the existing academic literature (Dudhwala 2020; Information Commissioner's Office 2021; Connon et al 2023). A summary of the findings of the review for LFR is shown below (Table 1).

Table 1: Summary: Live Facial Recognition Technologies

Summary: Live Facial Recognition Technologies	
Number of Documents that Discuss Live (Intelligent) Facial Recognition Technologies n=51	
Document Type	
Research Report	n=13
Conference Proceedings	n=2
Chapter from Edited Volume	n=1
Journal Article:	n=35
• Intersection of Science and Technology Journals	n=11
• Journals focusing on Law and the Application of Law	n=6
• Intersection of Law and Technology	n=2
• Criminology and Policing Journals	n=9
• Information Communications Journals	n=1
• Scientific Development Journals	n=2
• Interdisciplinary Journals of Surveillance Studies	n=1
• Human Geography Journals	n=1
• Policy Journals	n=2

Discussion of Issues

Social and Ethical Issues:	n=32
• Trust	n=12
• Bias and discrimination	n=18
• Consent	n=6
• Privacy, freedom	n=18
• Lack of regulation and ethical guidelines	n=9
• Legitimacy of use	n-14
• Normalisation of surveillance	n=6
• Security of data	n=7
• Access control	n=8
• Accuracy	n=11
• Biodeterministic forms of criminalisation	n=1
Suggestions to mitigate social and ethical challenges	n=14
Evidence:	
• Survey data	n=3
• Case study	n=9
• Analysis of existing literature	n=17
• Interviews	n=1
• Analysis of Legal documents	n=2
Legal Issues	n=11
• Human Rights and Equality	n=11
• Data Protection	n=8
• Necessity and Proportionality	n=1
• Choice	n=1
• Watchlist Generation	n=1
• Weaknesses in EU General Data Protection Register	n=1
• Protection of Vulnerable People and Children	n=1
• Potential Impact of Proposed EU AI Regulations	n=1
• Potential challenges to the boundaries of Criminal Procedure Act 1995	n=1
Suggestions/ to mitigate legal challenges	n=4
Evidence:	
• Existing Literature	n=3
• Case Law Review	n=6
• Survey Data	n=1
• Interviews	n=1

SECTION 2. BEHAVIOUR & EMOTIONAL AI IN LAW ENFORCEMENT

SECTION 2. BEHAVIOUR & EMOTIONAL AI IN LAW ENFORCEMENT

Introduction

The types of biometric identification technologies explored were the use of voice and gait recognition, signature (writing) identification, body movement and micro expression identification technologies. Each of these technologies involves the use of algorithms and identification based on human behavioural and emotional characteristics. Emotion and behaviour recognition algorithms aim to recognise, infer and harvest emotions using data sources that include voice, facial expressions, movements, gestures, and gait. This data is harvested in ways that are often opaque to the people providing these data (Andalibi and Buss 2020). From the algorithms developed based on this data, emotional and behavioural recognition technologies aim to detect and infer emotional stated. Emotional AI technologies recognise and classify emotions in the same way as behavioural characteristics which are more outwardly visible, and thus blur the boundary between the private and public expression of the self. The development of these technologies is rooted upon developments in Affective Computing in the 1990s and much of the emotion recognition research in technology and computing draws on the work of Ekman who identified six basic and universal human emotions: anger, disgust, fear, joy, sadness, and surprise. This is despite the fact that Ekman's work has been criticised by researchers who question the universality of emotion, arguing that there is not enough scientific evidence that a person's emotional stated can be readily inferred from facial or bodily movements or from their voice (Abdulrahman and Alayani 2021; Andalibi and Buss 2020).

3.1.1: Social and ethical issues

A number of social issues were identified with the different types of behaviour and emotion recognition technologies discussed in the sample literature.

3.1.1.1: Intelligent writing recognition technologies

One article discusses the social and ethical issues involved in the use of live signature/writing biometric technologies for law enforcement and protection, particularly in the prevention of crime (Abdulrahman and Alayani 2021). Signature recognition technologies perform live online handwriting checks where a person's signature is captured on a special pen which also detects pen location, physical force, angle, and the time elapsed in signing. However, these technologies require 5-10 or more examples of a user's signature to learn the intrapersonal fluctuations adequate to perform a precise check of a person's personality. These technologies can be prone to error owing to how their sensitivity and functionality can be affected by oil, dust, and water on the surface (ibid). They also require large databases to enable signature recognition which raises concerns about the safety of data storage (ibid). In addition, there is also the potential that these technologies may be vulnerable to being used for forgery, raising concerns about their vulnerability for use for nonlegal purposes (ibid).

Possible solutions

The Abdulrahman and Alayani (2021) article also suggested one possible solution to help address the issues and challenges identified in the use of this technology. It suggested that the

simultaneous use of different biometric AI technologies – fingerprint, voice, and signature – as part of a multimodal system of biometric identification may help to mitigate the potential issues and vulnerabilities (ibid). However, it also acknowledged that the use of multimodal systems would require further research and testing to explore to what extent they may be useful in overcoming such limitations (ibid).

3.1.1.2: Live voice recognition technologies

Seven documents specifically referred to the use of voice recognition technologies as part of biometric AI behavioural and emotional recognition systems (Connon et al 2023; McKendrick 2019; Jansen et al 2021; Podoletz 2022; Pal et al 2021; Mohamed et al 2020; and Abdulrahman and Alayani 2021). For example, Jansen et al (2021) explored the use of voice recognition in policing by looking at the case of the recent Speaker Identification Integrated Project, which was a European-wide initiative designed to develop the first interoperable database of voice biometrics. Podoletz (2022) focused on the issues surrounding voice in predicting crime and in the detection of deception, and Pal et al (2021) examined the use of voice recognition technologies as part of a larger suite of interactive human emotion recognition systems. Mohamed et al (2020) discussed the racial and ethnic biases inherent in live voice recognition technologies, as well as other forms of live biometric technologies and suggested ways that these biases may be overcome in future developments. Abdulrahman and Alayani (2021) explore the use of voice recognition technologies in automated decision making processes for crime prevention and outline the pros and cons of the use of these technologies for law enforcement practice.

These seven documents discuss a number of social and ethical issues associated with this type of technology: accuracy and performance; bias; consequences of dependency on automated decision-making; impacts on privacy and freedoms; and the risks associated with a lack of clear regulation of this type of technology.

Three of the articles discuss the issue of **accuracy and performance** (Podoletz 2022 and Abdulrahman and Alayari 2021, Jansen et al 2021). For example, Abdulrahman and Alayari (2021) explain that live voice recognition technologies are less reliable than live fingerprint recognition technologies and therefore may result in inaccuracies which can undermine public trust in the use of the technology. They explain that voice is not steady and is changeable with age. However, it can be difficult to imitate, meaning that it is less prone to manipulation than other forms of biometric identification systems. Similarly, Jansen et al (2021) explain that voice recognition technologies are prone to high error rates and environmental interferences can make them particularly unreliable.

Another issue noted is that of **privacy and data security** as voice recognition systems also require a large amount of data to be stored on large databases (Abdulrahman and Alayari 2021; Connon et al 2023; Pal et al 2021, Podoletz 2022, Jansen et al. 2021). For example, Pal et al. (2021) explore the use of voice recognition within interactive human emotion recognition systems and argued that because these technologies require large scale databases, it can make the protection of individual's privacy a challenge. In addition, there are also issues related to maintaining the security of data and of establishing access control requirements, as breaches of data pose major challenges for maintaining public trust. Jansen et al. (2021) explain that voice recognition technologies raise concerns relating to individual rights and freedoms of expression as well as for social justice because voice is the means by which people make themselves heard. They explain that these technologies may be problematic owing to their potential ability to silence voices because of their actual or perceived increased surveillance and policing of voices and human expression.

Inbuilt biases, particularly racial and gender biases, also pose another ethical problem which are associated with this type of technology (Connon et al 2023; Mohamed et al 2020; Podoletz 2022, Jansen et al 2021). For example, Mohamed et al. (2020) explain that vulnerable people including racial and ethnic minority groups are more likely to bear the brunt of the negative impacts of innovation and scientific developments in AI as voice recognition systems are less likely to be able to manage accent detection with accuracy, resulting in the risk of further alienating already socially marginalised groups and intensifying distrust in official institutions. They explore how values and socially-embedded unequal power dynamics shape the development and implementation of biometric AI technologies and outline how voice recognition systems, as well as other biometric tools, can result in algorithmic discrimination, algorithmic oppression, algorithmic exploitation and algorithmic dispossession – all of which relate to the issues of fairness and equality within these technologies and in their use. Similarly, Jansen et al. (2021) explain that inbuilt biases can affect the cross referencing of voices against a database of human suspects. These authors explain that the 'prototypical whiteness' and 'maleness' makes the genealogy of these biometric techniques suspect and leads to the misidentification of accents and voices outwith the dominant social group, leading to larger rates of misidentification amongst women, ethnic minorities and non-binary identities. This can lead to increased police surveillance of these groups and the implementation of inappropriate police action. Jansen et al. (2021) explain that biases undermine the legitimacy of the use of these technologies and argued that biometric technologies rely on a relatively narrow set of criteria that are unlikely to be able to match the cultural and social diversity of the general population, thus risking increased stereotyping and observation of specific communities.

Jansen et al. (2021) also explore the issues associated with the potential consequences of an increased dependency on automated forms of decision making in relation to voice recognition technologies. They highlight the ethical issue of algorithmic doubt and certainty. This refers to how algorithmic systems can potentially erase the presence of doubt in decision making, whilst simultaneously generating the parameters against which uncertainty will be judged, further raising the possibility of error and inaccuracy.

Two documents explore how concerns related to security and the lack of clear regulatory standards result in these technologies being deemed problematic (Connon et al 2023; McKendrick 2019). For example, McKendrick (2019) arguedd that voice recognition technologies are associated with concerns regarding human rights and a lack of well-established norms governing the use of AI technology in practice.

Possible solutions

Two of the articles explore potential solutions or ways of mitigating the challenges and negative impacts of these technologies on society (Mohamed et al 2020; Abdulrahman and Alayari 2021). Abdulrahman and Alayari (2021) explain that the combined use of different forms of biometric technologies can help to prevent inaccuracies, which in turn, may help to establish, maintain or restore public confidence and trust in these technologies. However, they also stated that further research is required to explore the extent to which the combined use of technologies can actually help to reduce the rates of errors and inaccuracies. Mohamed et al (2020) explore how decolonising AI may help mitigate the issue of racial and ethnic bias. They explain that this will require improved aligning of research and technical development and the development of ethical principles to improve algorithmic fairness. They also argued that the development of these principles used to guide technological development and implementation needs to involve greater integration between policy, research, technology developers and the public. This helps to ensure improvements in public trust and legitimacy as well as to improve the equality of accuracy embedded in these systems and their use. None of the articles explore potential solutions to

the issues surrounding privacy and the maintenance of data security or ways of mitigating the negative consequences associated with dependency on automated forms of decision making.

3.1.1.3: Gait recognition technologies

Only one article within the sample discusses the algorithmic use of gait recognition technologies (Harris et al. 2022). Harris et al (2022) arguedd that these technologies involve the use of human pose tracking with one-person or multi-person tracking systems. They explain that these technologies are useful for person identification, authentication, and re-identification in law enforcement. Abnormal gait detection can be useful for fraud detection, impersonation and also for the detection of persons under the influence of alcohol or substances (ibid). They argued that gait detection technologies present greater reliability than other forms of behaviour and emotional detection, because the individuality of gait pattern persists over time and over many pathologies (ibid). However, the accuracy of the algorithm that the use of these technologies depend upon may be called into question owing to limitations in the sample size that these technologies are developed from (ibid). Other important social and ethical issues associated with gait recognition technologies are those of increased surveillance creep and legitimacy of use (ibid).

Possible solutions

No solutions to the social and ethical challenges identified were posed.

3.1.1.4: Body language and micro expression identification technologies

Six of the documents reviewed explored the use of body language and micro expression identification technologies in law enforcement (Jupe and Keatley 2020; Pawels 2020; Wright 2021; Andalibi and Buss 2020; Claypoole 2021; and Barkane 2022).

Five of these documents identified social and ethical challenges associated with the use of these technologies (Jupe and Keatley 2020; Pawels 2020; Wright 2021; Andalibi and Buss 2020). One of these challenges is the **risk of misidentification and false detection** associated with these technologies owing to the complexity and diversity of emotional expression. This can undermine public trust and confidence in these technologies, which was identified in two of the documents (Jupe and Keatley 2020 and Andalibi and Buss 2020). Jupe and Keatley (2020) explore the ethical issues associated with body language recognition systems, especially in their ability to identify people and to detect deception. These technologies are based on detecting and measuring gaze aversion, fidgeting, postures, and facial expressions. However, they argued that reliance on nonverbal cues for identification and detection is unreliable, because physical responses to emotional stimuli are difficult to standardise in algorithms, depending on large samples to account for human diversity to prevent misidentification and false detection. Similarly, Andalibi and Buss (2020) argued that emotions can be complex and difficult to define, leading to a lack of trust in algorithms.

Another challenge is **establishing and maintaining legitimacy**. Wright (2021) explored the ability of emotional recognition AI systems based on micro expressions and body language to quantify a subject's mental and emotional stated. Wright (2021) argueds that the use of these technologies can result in subjects being unnecessarily treated with suspicion or as potential criminals, which can fix identities as 'deviant' and 'criminal', thus creating concerns relating to control over subjects.

The third issue identified was that of the **impact of these technologies on people's sense of privacy over matters considered to be private**. Andalibi and Buss (2020) explain that emotions

are deemed to be private and technologies that aim to detect an individual's emotional stated bring private emotions into the public space for scrutiny. They explain that there are both personal and collective risks relating to the issue of privacy in the use of emotional AI technologies (ibid). The personal risks range from increased risks of control, manipulation, exploitation, identity misrepresentation (including beyond a person's lifetime), to negative mental health impacts associated with increased surveillance as well as availability of sensitive mental health related data given that these systems can be used to detect a person's mental health status (ibid). Collective risks include the risk of political control and manipulation (ibid).

Another concern associated with the use of these technologies is the **lack of public support** and the lack of guidelines concerning their ethical use. Andalibi and Buss (2020) explain that from a national survey of public attitudes in the UK towards the use of these technologies, over 50% of respondents were uncomfortable with the use of emotional AI and emotional recognition technologies and only 8.6% were comfortable with their use if the inferences could be linked back to them. They also explained that public support was different in the UK compared to the US due to differences in privacy norms and political ideologies that inform policy attitudes. However, in both countries support was greater amongst people who were wealthy, male, educated or skilled in the use of technologies (ibid).

The fifth ethical concern identified in two sources is that of **data storage and data sharing practices**, namely the potential consequences of the lack of consensus and regulation over these issues (Andalibi and Buss 2020; Pawels 2020). Potentially, the lack of regulation could result in abuses of Human Rights through increasing forms of censorship and surveillance in public spaces (Pawels 2020). Andalibi and Buss (2020) explain that concerns with this type of technology relate to how data concerning emotional stated should be treated as sensitive data owing to their connection with an individual's mental health status.

Possible solutions

Only one article (Andalabi and Buss 2021) discusses potential solutions to challenges identified, but only does so in relation to two of challenges – the challenge of establishing and maintaining public trust in use of these technologies and the challenge of safeguarding the data associated with these technologies. They argued that ethical guideline development for the use of these technologies needs to take place early on the process of algorithm development and must involve shared consensus concerning their use by all developers, users and third parties (ibid). They also argued that the data captured should be considered as sensitive data to ensure stricter safeguarding and access requirements are upheld by all parties.

3.1.2: Legal issues

None of the documents in the sample discussed the legal issues and implications associated with intelligent writing recognition technologies, suggesting a potential area for further research and consideration. Similarly, none of the articles directly discussed the legal issues and implications associated with live voice recognition technologies or the use of gait recognition technologies.

Three of the documents reviewed discuss the legal issues relating to biometric body language and micro expression identification technologies (Barkane 2022; Pawels 2020, and Claypoole 2021). The main legal challenges that these forms of technologies pose lies in their potential to harm human rights if misused and the difficulties ascertaining responsibility for these harms (Pawels 2020; Claypoole 2021; and Barkane 2022). This can result in the creation of an accountability gap, making it difficult for injured parties to be able to access a remedy or receive fair treatment by

the justice system (ibid). Another concern is that the use of these technologies could potentially weaken the international rule of law through facilitation of extrajudicial actions (Pawels 2020).

The specific rights identified that the unregulated use of these technologies may potentially threaten are the right to privacy, the right to self-determination, the right to freedom of expression, and non-discrimination and minority rights (Pawels 2020; Claypoole 2021; Barkane 2022).

Two articles discuss the limitations of existing and proposed regulation and legislation concerning the application of these types of biometric AI (Claypoole 2021; Barkane 2022). Claypoole (2021) argueds that US legislation should limit the application of biometric AI technologies within constitutional bounds owing to the capacity of these technologies to potentially undermine privacy and constitutional rights. Barkane (2022) questions the efficiency of the proposed EU AI Act for addressing the threats and risks to fundamental rights posed by these types of identification and surveillance technologies. The Act proposes to prohibits the use of real time remote biometric identification technologies in publicly accessible spaces for law enforcement purposes, but the specific time lag that their use can involve is not specified directly or clearly enough (ibid). Nor does the act specify what can happen in private spaces, such as in homes. Emotional and behavioural recognition technologies can however still be used in real time for targeted searches for potential victims and perpetrators of crimes and for the prevention of imminent threats to physical safety. These technologies can also be used for the identification and persecution of suspects wanted for criminal offences on issue of a European arrest warrant if the offenses are punishable in a particular member stated by a custodial sentence or detention order for at least three years (ibid). However, what is meant by 'strictly necessary' purposes is too ambiguous to provide proper clarity over the issue. However, none of these articles focus on the legal issues that emerge within a Scottish or UK context.

Possible solutions

Two of the articles discuss possible solutions to the legal challenges identified (Pawels 2020; Barkane 2022). Pawels (2020) arguedd that there is a need to devise a Theory of Harms in AI space as a means of developing an adequate method to weigh the benefits of these technologies against the potential harms to Human Rights and civilian security. In addition, to address the accountability gap, a cross-sector collaboration to identify potential anticipated misuses should be undertaken, as well as to discuss the long-term impacts of AI and data capture technologies on vulnerable populations. In addition, a Human Rights impact assessment should be undertaken prior to the trials as well as the implementation of these technologies. Remedy mechanisms should also be established and clarified (ibid). Barkane (2022) argueds for the use of cross party conformity assessments, fundamental rights impact assessments, transparency obligation agreements as well as for the enhancement of the existing EU data protection law and rights and remedies available to individuals subjected to harm. However, once again, neither of these articles focus on Scotland or the wider UK.

Evidence base

Out of fifteen documents reviewed, ten drew on evidence from the existing literature, with just one (Jansen et al. 2021) drawing on primary data from a specific case study. One included evidence drawn from survey and interview data (Andalibi and Buss 2020), one drew on historical data (Wright 2021) and two drew upon legal documents and statutes (Barkane 2022, and Claypoole 2021). A Summary of the findings for behaviour and emotional recognition technologies is shown in Table 2.

Table 2: Summary: Behaviour and emotional recognition technologies

Summary: Review of Behaviour and Emotional Recognition Technologies				
Number of Documents focusing on Intelligent Behaviour and Emotional Recognition Technologies n=14				
Document Type				
Research Report Conference Proceedings Journal Article: • Science and Technology Journals • Security Studies Journals • Information and Communications Technology Journals • Legal Journals • Interdisciplinary Journals: Science, Technology and Society Journals	n=2 n=1 n=11 n=3 n=2 n=1 n=1 n=4			
Issues By Technology Type				
	Live voice recognition n=7	Gait recognition n=1	Body language and micro-expression n=6	Writing recognition technologies n=1
Social and Ethical Issues: • Accuracy • Bias and discrimination • Dependency • Privacy, freedom • Lack of regulation and ethical guidelines • Legitimacy • Surveillance • Security	n=7 n=3 n=4 n=1 n=5 n=2 n=0 n=0 n=0	n=1 n=1 n=0 n=0 n=0 n=0 n=1 n=1 n=0	n=5 n=2 n=0 n=0 n=1 n=1 n=1 n=0 n=1	n=1 n=1 n=0 n=0 n=1 n=0 n=0 n=0 n=0
Suggestions to mitigate social and ethical challenges				
Evidence: • Existing literature • Case study • Historical documents • Survey & Interviews • Legal document analysis	 n=6 n=1 n=0 n=0 n=0	 n=1 n=0 n=0 n=0 n=0	 n=2 n=0 n=1 n=1 n=1	 n=1 n=0 n=0 n=0 n=0
Legal Issues				
• Human Rights • Weakening international rule of law • Limitations of existing law	n=0 n=0 n=0	n=0 n=0 n=0	n=1 n=2 n=1	n=0 n=0 n=0
Suggestions/ to mitigate legal challenges				
Evidence: • Legal document analysis (case law) • Existing Literature	 n=0 n=0	 n=0 n=0	 n=2 n=1	 n=0 n=0

SECTION 3. FORENSIC DNA PHENOTYPING TECHNOLOGIES IN LAW ENFORCEMENT

SECTION 3. FORENSIC DNA PHENOTYPING TECHNOLOGIES IN LAW ENFORCEMENT

Introduction

Fifteen documents within the sample explored the use of DNA predictive phenotyping technologies in law enforcement. DNA profiling is another tool available to police for criminal investigation (Ahuiri-Driscoll et al 2021). Forensic DNA phenotyping refers to the prediction of appearance traits of unknown sample donors or unknown deceased or missing persons, directly from biological materials found at a scene (Kayser 2015). It can provide investigative leads to trace unknown people who are unidentifiable with comparative DNA profiling. This intelligent application of DNA represents an established but still evolving field of DNA testing (Atwood et al 2021). Certain group-specific pigmentation traits are predictable from DNA, and forensic DNA profiling aims to infer an unknown person or sample donor's externally visible characteristics (EVCs) from DNA (or other molecular biomarkers) directly from the biological material left behind at the crime scene (ibid). It therefore provides intelligence regarding the appearance (externally visible characteristics), biogeographical ancestry and age of an unknown donor. As Keysar (2015) notes, forensic DNA profiling outcomes can serve as a 'biological witness' and can provide investigative leads enabling the tracing of unknown perpetrators of crime. It can therefore assist law enforcement agencies by re-prioritising an existing pool of suspects or generating a new pool of suspects (Atwood et al. 2021; Albrecht 2020)

The DNA inference of bio-geographic ancestry (BGA) is sometimes considered part of forensic DNA profiling, however genetic ancestry does not always portray an externally visible (phenotypical) characteristic, particularly in individuals of mixed genetic ancestry (Keyser et al 2015). A notable difference with inferring bio-geographical ancestry (BGA) and externally visible characteristics (EVCs) of an unknown individual is the capacity to provide DNA information in an investigation to assist with individual identification by generating leads without reliance on the availability of a comparison sample. Such intelligence can also be applied to cold cases, unidentified human remains cases and disaster victim identification; all scenarios where the success of short tandem repeats (STR) identification can often face additional limitations due to degraded, or poor quality, biological evidence.

Prediction accuracy is essential for confidence in result outcomes when applying forensic DNA phenotyping to police casework. The use of relevant and informative DNA markers for the traits of interest is of paramount importance. Secondly, the composition of the reference set that is used to train the algorithms analysis must be appropriate and relevant for the predictive trait. The populations contained within these datasets are often unknown to the user or may vary considerably in their representative construct applicable to the trait being tested. In addition, the accuracy of the prediction is dependent on the prediction algorithm used. At present, only a handful of software have been developed which are capable of analysing the data to produce outputs about likely physical traits. These are IDentity, Indentitas, and SNaPshot Software by Parabon NanoLabs (Vajpayee and Shukla 2021).

Of the fifteen documents reviewed in this study, 12 were peer-reviewed articles from academic journals (Ahuriri-Driscoll et al 2021; Albrecht 2020, Atwood et al 2021; Hopman 2020; Katsara et

al 2021; Kulka-Barteszele et al 2019; Machado and Silva 2019; Miller and Smith 2022; Murphy 2018; Queirós 2019; Samuel and Prainsack 2019; Scudder et al 2019). Two were government and policy-relevant research reports (Presser and Robertson 2021; Samuel and Prainsack 2018). One was a peer reviewed book chapter from an academic edited volume (Vajpayee and Shukla 2021).

3.3.1: Social and ethical issues

Thirteen of the fifteen documents reviewed discussed the social and ethical issues associated with this type of technology (Ahuriri-Driscoll 2021; Atwood et al 2021; Hopman 2020; Katsara et al 2021; Kulka-Bartoszek et al 2019; Miller and Smith 2022; Machado and Silva 2019; Murphy 2018; Presser and Robertson 2021; Queiros 2019; Samuel and Prainsack 2019; Scudder et al 2019; Vajpayee and Shukla 2021).

One of the key social and ethical issues identified was that of the **potential for discrimination of minority racial and ethnic groups** through the use of these technologies (Ahuriri-Driscoll et al 2021; Atwood et al 2021; Murphy 2018; Presser and Robertson 2021; Queiros 2019; Samuel and Prainsack 2019; Scudder et al 2019; Vajpayee and Shukla 2021). Concerns about discrimination resulting from these technologies pertain to 1) the differentiating power of externally visible characteristics, 2) incorrectly assumed differences in accuracy between genetic and eyewitness testimonies, and 3) the collectivisation of suspicion (Queirós 2019). As Queirós (2019) arguedd, the differentiating power of forensic DNA phenotyping renders race and ethnicity visible through the racialisation of specific physical appearance traits. This means that some groups remain invisible, while others are 'phenotypically othered' and become more frequent suspects of police surveillance and community suspicion. Similarly, Ahuriri-Driscoll et al (2021) arguedd that the use of these technologies and methods may increase Indigenous and racial minorities' experiences of criminalisation in New Zealand through the risk of aggravating existing police biases and over-scrutiny of Indigenous minorities who are more likely to be apprehended and arrested. Harmful assumptions that Indigenous people are predisposed to criminality and arrest for criminal offending may inform the use of these technologies and may also ultimately be realised through prejudicial police practices, creating a self-fulfilling prophecy that reinforces these assumptions (ibid). Racial stereotypes may drive over-targeting for DNA sampling by police, leading to the over-representation of minorities in DNA profile databases from which algorithmic predictions are then based upon. In addition, as Hopwood (2020) notes, the results of these predictive approaches are more efficient when they point at a minority population within a particular geographic context. The potential for over-policing amongst minority populations through the use of this method could exacerbate existing social tensions between the police and minority groups and also between minority groups and the dominant social group (ibid; Queirós 2019). Furthermore, as Presser and Robertson (2021) explain, not only do the predictive algorithms that these technologies rely on inbuilt biases owing to the over-representation of members of racialised communities in the criminal justice system, but those also most likely to be identified using predictive technologies are often the least financially able to challenge it within the courtroom.

Another concern relating to the issue of discrimination was that of the **risk of greater miscarriages of justice** against the socially marginalised, as well as the risk of increased conflict between social groups, as a result of jurors and members' of the public's beliefs in DNA evidence as being 'fool-proof and incontrovertible' and because they subsequently base their decisions regarding guilt on the basis of misassumptions about the accuracy of predictive DNA phenotyping evidence alone (Ahuriri-Driscoll et al 2021; Murphy 2018; Queirós 2019).

A third issue identified relating to the issue of **discrimination** is that the method itself can also contradict with culturally specific beliefs surrounding the body, identity and group membership, and rights (Ahuriri-Driscoll et al 2021). For example, Ahuriri-Driscoll et al (2021) arguedd that

genetic material holds particular significance for Indigenous people in New Zealand and Australia for establishing identity and group membership. Its taonga (treasure) status among Māori people entail particular sensitivities regarding its handling and use. The Māori have specific cultural meanings associated with DNA and genetic material, as "a physical manifestation of valued metaphysical life forces [that] can be deemed to be collective cultural property" (p. 250) which correspond with traditional beliefs that by taking a physical part of a person, a part of that person's spirit is also taken, which could be used to create harm to or misfortune for or to that person.

Another major social and ethical issue associated with this technology was that of its **accuracy**, (Alhuriri-Driscoll et al 2021; Atwood et al 2021; Hopman 2020; Katsara et al 2021; Murphy 2018; Samuel and Prainsack 2019; Scudder et al 2019; Vajpayee and Shukla 2021). Atwood et al (2021) explain that although the predictive approach can provide accurate predictions of an unknown individual's EVCs and BGA, service providers differ in their testing approach and reference sets used, which may be reflected in the outcome and the prediction accuracy. In addition, the translation of scientific outcomes of FDP to lay audiences has been shown to be variable, which has meant that lay audiences do not always fully understand the limits of this method, which can have implications for decision making as well as for the social acceptability of these technologies (ibid). In particular, more extensive research and development are required to increase the prediction accuracies of skin colour and age (ibid). In addition, while donor samples received by service providers may be pristine, samples routinely encountered in law enforcement casework are more likely to be of compromised quality and even less likely to generate accurate results (ibid; Murphy 2018). Another important issue is that of a lack of understanding of the science between BGA assessments and an individual's actual physical appearance (Atwood et al 2021). Prediction of the BGA from a sample is not the prediction of race, ethnicity, or cultural background per se. Rather, it provides a prediction of the ancestral geographic or sub-geographic region of that sample. Lack of awareness of this fact in law enforcement is problematic because although the affiliation between BGA prediction and assumption of physical appearance may align, BGA prediction does not imply the actual physical appearance of a person (ibid; Samuel and Prainsack 2019). In addition, as Katsara et al (2021) stated, currently available models on appearance genetics remain incomplete and do not include all causal genetic variants as predictors. Furthermore, while trait prevalence-informed priors (for eye, hair and skin colour, hair structure and freckles) may have an effect on prediction performance, the rate of effect can vary, with some categories barely showing an effect (ibid). Also, misspecification of priors can diminish the accuracy of performance. This shows the importance of the degree of accurate specification of prevalence-informed priors required for prediction modelling of appearance traits. However, current limitations on these models mean the methods are not as accurate as people tend to assume (ibid; Samuel and Prainsack 2019; Scudder et al 2019). Kulka-Bartoszek et al (2019) looked at the prediction accuracy of these technologies for determining the presence of freckles, as a physical trait, and found that false positive predictions were high because the freckle phenotype in childhood can disappear in adulthood. They argued that predictions need an accuracy threshold as at present there is no standardised threshold and confusion about what counts as an accurate result can lead to law enforcement officials, jurors, and members of the public putting too much faith in the performance accuracy of these technologies (ibid). As explained by Samuel and Prainsack (2019), at present the scientific accuracy of these methods is not yet reliable enough and that there is no one 'toolbox of method' that can be applied and defined as FDP.

Another important social and ethical issue discussed in the sample literature related to the **storage of the large amounts of data required to enable the use of this form of technology and the risk of security breaches** (Hopman 2020; Scudder et al 2019; Vajpayee and Shukla 2021). Hopman (2020) arguedd that this technology relies on large data banks because, in order to get closer to genetically accounting for facial variation, researchers require larger and larger

amounts of biometric data. This can lead to increased risks and concerns regarding the impacts of a potential breach of the databanks where this data is held (ibid).

Concern over privacy of biometric information, the potential for improper use of forensic DNA genetic data and limitations over data access specifications represent another major social and ethical implication discussed in the sample literature (Machado and Silva 2019; Samuel and Prainsack 2019; Scudder et al 2019; Vajpayee and Shukla 2021; Miller and Smith 2022). Machado and Silva (2019) explain, using the findings from a survey about public attitudes towards DNA databases and technologies, that members of the public are highly concerned about data storage by law enforcement and potential for access by third parties. They also explain that, coupled with this, are concerns over the lack of discussion about whether police should be able to access data held by personal genetic services, including genetic genealogy databases for generating investigative tools, which represents another area of concern (ibid). Samuel and Prainsack (2019) also discuss the political and societal sensitivity of ancestry testing because the majority of the public and law enforcement officers perceive this information to be ethically, politically and socially sensitive, and explain how these concerns rose as a result of political actors linking the expanded use of DNA-testing to the topic of migration in scientifically and politically problematic ways. Others were concerned about access to and use of genetic markers related to predispositions of disease (ibid), with one concern being that even if health was not used as part of the predictive modelling process, information could still be produced and stored about an individual's health or medical predisposition as an 'incidental finding' (ibid). This could happen if the marker for the tested trait is in close proximity to a marker for a specific health pre-disposition (ibid). However, as Miller and Smith (2022) note, although the right to privacy is not absolute, people could arguably have the right for law enforcement agencies not to access their genetic data. This could be overridden under certain circumstances, such as in the case of a serious crime and then only for the purpose of identifying persons who have committed the specific crime. However, moral questions arise over the justification for the potential retention of DNA profiles of innocent people or suspects not subsequently convicted of a crime (ibid).

Another ethical issue identified by just one of the documents within the sample (Miller and Smith 2022) was the issue of joint moral rights in relation to the use of this form of technology. As Miller and Smith (2022) explain, the genome of a person is not only constitutive of that person's individual-specific (biological) identity because that same genome is in part constitutive of the individual-specific (biological) identity of a person's relatives. Therefore, it could be arguedd that the right to control one's genome data should be regarded as a joint right (held with an individual's relatives) rather than as an individual right. If it can be regarded as a joint right, then it follows that an individual may not have an exclusive individual right to provide his or her data to law enforcement (ibid). In cases where identifying the person who has committed a crime relies on the genomic data of relatives known to be innocent and the relatives in question have a joint right to the data in question, then it can be questioned whether all relatives need to have consented to the collection of the genomic data in question (ibid).

Another ethical consideration posed by this type of technology and discussed in one of the articles was the **right not to self-incriminate** (Miller and Smith 2019). The privilege against self-incrimination entitles a person to refuse to answer any question, or produce any document, if the answer or the production would tend to incriminate that person. (ibid). It can be arguedd that legally requiring a person to provide DNA evidence which, when using predictive forms of DNA phenotyping may result in them inculpating themselves in the future, is a breach of the legal privilege not to self-incriminate. This legal privilege is based on the moral right not to self-incriminate and which is closely related to the right to self-defence (ibid).

A final ethical issue raised by this type of technology is that of the issue of **collective moral**

responsibility. This was also raised in one article (Miller and Smith 2022). Public programs of DNA collection, such as mass collection programs implemented in China, enable all citizens to be identified in a criminal investigation if necessary (ibid). If we apply the concept of collective moral responsibility to the access of genomic information by law enforcement agencies to investigate and prosecute crime and, in particular, to universal DNA databases, it can be arguedd that there is a collective good to which the use of this information can make to law enforcement, namely, the investigation and prosecution of serious crimes. It could therefore be arguedd that there is a collective moral responsibility on the part of members of the stated to submit their DNA (ibid). However, it can also be arguedd that the collective moral responsibility applies only in specific cases and not to provide DNA data to contribute to a universal or quasi-universal DNA database (ibid). In addition, it can be arguedd that there cannot be a collective moral responsibility to provide DNA on a permanent basis (ibid).

Possible solutions

Three of the articles offer and discuss possible solutions to some of the social and ethical challenges associated with this type of technology (Ahuriri-Driscoll et al 2021; Atwood et al 2021; Scudder et al 2019).

Ahuriri-Driscoll et al (2021) argued that the problem of racial and ethnic discrimination associated with this form of technology may be reduced through a wider effort to decolonise criminal justice. However, they also explain that greater consideration needs to be given as to what a decolonised criminal justice system and process may look like as well as to how it can be successfully implemented (ibid). Atwood et al (2021) argueds that concerns over a lack of public, juror and law enforcement professional understanding of the actual real-world accuracy of the outcomes of these technologies could be reduced through improved communications from developers written in clear and concise language so as to ensure they are comprehensible by a non-expert/ lay audience. They also arguedd that in criminal investigations, performance should be assessed by scientific experts so as to ensure that the outcomes do not require interpretation by the lay audience (ibid). Limitations of the accuracy of the technologies and outputs should be clearly indicated (ibid). In addition, the service providers should provide the genotype data generated for every test undertaken to allow for independent verification of the results (ibid). Scudder et al (2019) argued that challenges resulting from misunderstandings about the accuracy of this technology may be mitigated by developing and applying an appropriate intelligence doctrine or framework that outlines the current and emerging capacities of these technologies in the context of law enforcement use.

However, none of the documents reviewed offered possible solutions for mitigating the issues associated with potential security breach of data, potential for improper use, lack of clarity over third party access, as well as the questions raised concerning joint moral rights, the right not to self-incriminate and collective moral responsibility.

Evidence base

Out of the thirteen documents that explored the social and ethical issues associated with DNA phenotyping technologies, one was based on interview data from members of the public and those involved in law enforcement activities (Queiros 2019), while another was based on interview and focus group data (Ahuriri-Driscoll 2021). One was solely based upon interview data from participants who had a professional stake in FDP technologies (Samuel and Prainsack 2019). Three of the documents were based on case studies of the use of this form of technology in policing and law enforcement practice in Australia, Canada and the Netherlands (Atwood et al 2021; Hopman 2020; Presser and Robertson 2021), and one was based on the comparative

analysis of public survey data from members of the public in Italy, Portugal, Serbia, Spain, Switzerland, the USA and New Zealand (Machado and Silva 2019). Another four were based on existing scholarly data (Murphy 2018; Miller and Smith 2022; Scudder et al 2019; Vajpayee and Shukla 2021), with one of these including a review of case studies from the existing scholarly literature (Vajpayee and Shukla 2021). The two other documents were based on the outcome of laboratory-based studies (Kulka-Bartoszek et al 2019; Katsara et al 2021).

3.3.2: Legal issues

Six of the fifteen documents on DNA phenotyping, discuss legal issues associated with this technology (Ahuriri-Driscoll et al 2019; Albrecht 2020; Murphy 2018; Presser and Robertson 2021; Samuel and Prainsack 2018; and Vajpayee and Shukla 2021).

One of the legal issues discussed in relation to these technologies is the issue of **truthfulness and fairness** in the administration of procedural justice (Ahuriri-Driscoll et al 2019; Murphy 2018; Presser and Robertson 2021). Ahuriri-Driscoll et al (2019) argued that there is a risk of DNA evidence unduly influencing trial outcomes and perhaps even distorting justice due to its perceived infallibility and limited lay public understandings. Similarly, Murphy (2018) arguedd how judicial actions have been shown to have poor ability to discern between different types of DNA analysis techniques and how prosecutors have been susceptible to the myth of the infallibility of DNA. They explain that this can also lead to defense lawyers giving up in the face of seemingly indisputable DNA match without probing the reliability of the match further (ibid). Presser and Robertson (2021) call this presumptive inadmissibility in the absence of strict scrutiny and argued that one of the existing challenges is that novel forms of forensic evidence such as FDP are not properly entrenched in the legal system through the codification of common law principles. They argued that in the Canadian legal system, full adherence to placing the burden of proof on the moving party is particularly important to ensure that vulnerable defendants in the criminal justice system are not required to bear a heavy persuasive burden of showing the need for caution and strict scrutiny of novel, AI-based forensic methods.

The second issue discussed was the legal challenges associated with **personal data retention and analysis** for purposes of crime control (Albrecht 2020). Albrecht (2020) arguedd that both the Court of Justice of the European Union (CJEU) and the European Court of Human Rights stress the importance of efficient investigation and information gathering methods for security and for the prosecution of serious crime and therefore questions arise over whether an appropriate balance can be struck between the interest in security and effective prosecution on the one hand and fundamental rights on the other.

Vajpayee and Shukla (2021) identify two other important legal issues linked to the use of these technologies. The first is that it can lead to what they term **the Slippery Slope Theory**. According to this theory, since the FDP technology is very new, a lot of information is fed into the knowledge bank daily. This increases the scope of forensic DNA phenotyping technology in the future and this advancement in the capabilities of FDP could lead to the misuse of the information inferred (ibid). They argued that if accessing the information from one form of FDP is allowed, then eventually all forms of FDP could be used and controlling only a part of FDP to be used for information purposes will become a tough task (ibid).

The other legal issue identified in this article concerns **the right not to know** and the implications of these technologies for this right (Vajpayee and Shukla 2021). Within this an individual enjoys their rights not to know their own medical information. Thus, law enforcement investigation must be limited to analysis of physically visible traits. Advancements in the technology have claimed there is a potential relationship between genetic markers and behavioural traits of the individual,

and thus DNA testing could reveal behavioural aspects and relate them directly or indirectly to the person's criminal behaviour. This is concerning because if this information is revealed to the person or accepted by the court of law, it could affect parole eligibility and preventive detention (ibid). A person could also use this information to make an excuse for criminal actions (ibid).

Another issue concerns the legal aspects of regulation and governance of these types of technologies and, specifically, the **lack of clarity** over FDP in the existing legal framework. Samuel and Prainsack (2018) explain how the European Union's legal and regulatory framework, along with the legal and regulatory frameworks of eight European countries (including Austria, France, Germany, Poland, The Netherlands, Spain, Sweden, and The United Kingdom), accommodate the use of new forensic DNA phenotyping technologies. They also provide an overview of the legal permissibility and practice of FDP in EU member stated, as well as other countries of interest, including United States, South Africa, and Australia. They explain that one issue is that in the UK there is no explicit legislation governing which techniques can be used for forensic DNA analyses for crime scene DNA stains, with the legislation that exists covering only the collection, processing, and storage of DNA for forensic purposes. As such, according to the letter of the law, FDP is permitted. All statutory frameworks related to forensic genetic tests relate to the circumstances in which a sample can be taken from an individual, and the circumstances under which the findings of any forensic genetic tests conducted on the sample can be stored. The UK operates an adversarial legal system, and it is the police's role to gather evidence in a criminal case. As such, FDP can be requested by police and forensic providers at their discretion without formal requests being made to the courts (ibid).

Furthermore, any use of FDP or the storage of FDP findings would need to be GDPR and Police and Criminal Justice Data Protection Directive compliant (Samuel and Prainsack 2018). However, at present it is unclear when FDP findings become personal data and whether FDP findings should be given special category status because of their genetic nature. Greater clarity is also required about how long FDP findings should be stored and whether FDP would fall under extra legislation related to AI/automated decision-making given the use of algorithms in FDP tests (ibid). In the UK, analysis of the physical appearance of the perpetrator is allowed according to the existing legislation, but ethnic inference cannot be inferred (Vajpayee and Shukla 2021). However, at the same time, there is also no specific regulation forbidding FDP for age, appearance, or ancestry at present. In England and Wales, the Police and Criminal Evidence Act regulates the UK national DNA database and stated who can take a DNA sample from an individual, and under what circumstances, but this Act was written in the context of STR-DNA profiles only and does not discuss any other form of DNA finding or analysis such as FDP. Furthermore, while the Protection of Freedoms Act (POFA) 2012 stated the circumstances under which the DNA sample/data can be stored, for how long, and when it needs to be destroyed, again it was also developed in the context of STR-DNA profiling and contains no explicit regulation governing the storage of FDP findings in national databases (ibid).

Possible solutions

To improve the current lack of legal clarity surrounding the use of FDP technologies, Presser and Robertson (2021) explain drawing on evidence from the Canadian system, that governments should consider statutory amendments to prescribe the use of FDP systems and to promote their legal accountability.

In particular, they argued that amendments should focus on improving the use of DNA analysis as evidence and focus on enhancing systemic transparency and accountability surrounding the use of algorithms in criminal justice system to improve the perceived infallibility of FDP methods

and its impacts on fairness in the courtroom (ibid). They also argued for prescribed limits on the admission of AI-generated evidence in criminal proceedings, owing to the unique challenges associated with AI-evidence and the imbalance of power, knowledge, resources, and expertise between individual defendants in the criminal justice system and the developers of AI-based tools. They argued that AI-generated evidence should be considered expert opinion evidence and that requirements regarding the availability of human witness testimony in the courtroom should be carefully considered to address the unique challenges associated with AI-generated evidence (ibid). Government and law enforcement agencies that develop their own algorithmic technologies—whether in-house or with private vendors—should also be required to make the source code and related details of such technologies publicly available in machine-readable forms that can be understood by the lay reader. Prosecutorial guidelines concerning the use of FDP technologies in criminal proceedings should also be introduced to mandate a commitment to robust and full disclosure surrounding methods to defendants and their counsel (ibid). Training programs should also be developed for all justice-system participants to enable a comprehensive understanding of the nature of these technologies and their risks (ibid).

To improve the lack of legal clarity concerning the collection and storage and sharing of data, Presser and Robertson (2021) argued that systems of oversight concerning the collection, use, retention and sharing of DNA information within police investigations and criminal proceedings should be modernised to keep pace with advances in technology and to enable accountability surrounding the use of sensitive techniques (ibid). Legal reforms should also aim to facilitate public access to information regarding what DNA databases law enforcement authorities and forensic laboratories obtain access to, where DNA profiles are sourced from, and the relationship between private companies and public sector actors regarding the collection, sharing, and use of DNA profiles.

Evidence base

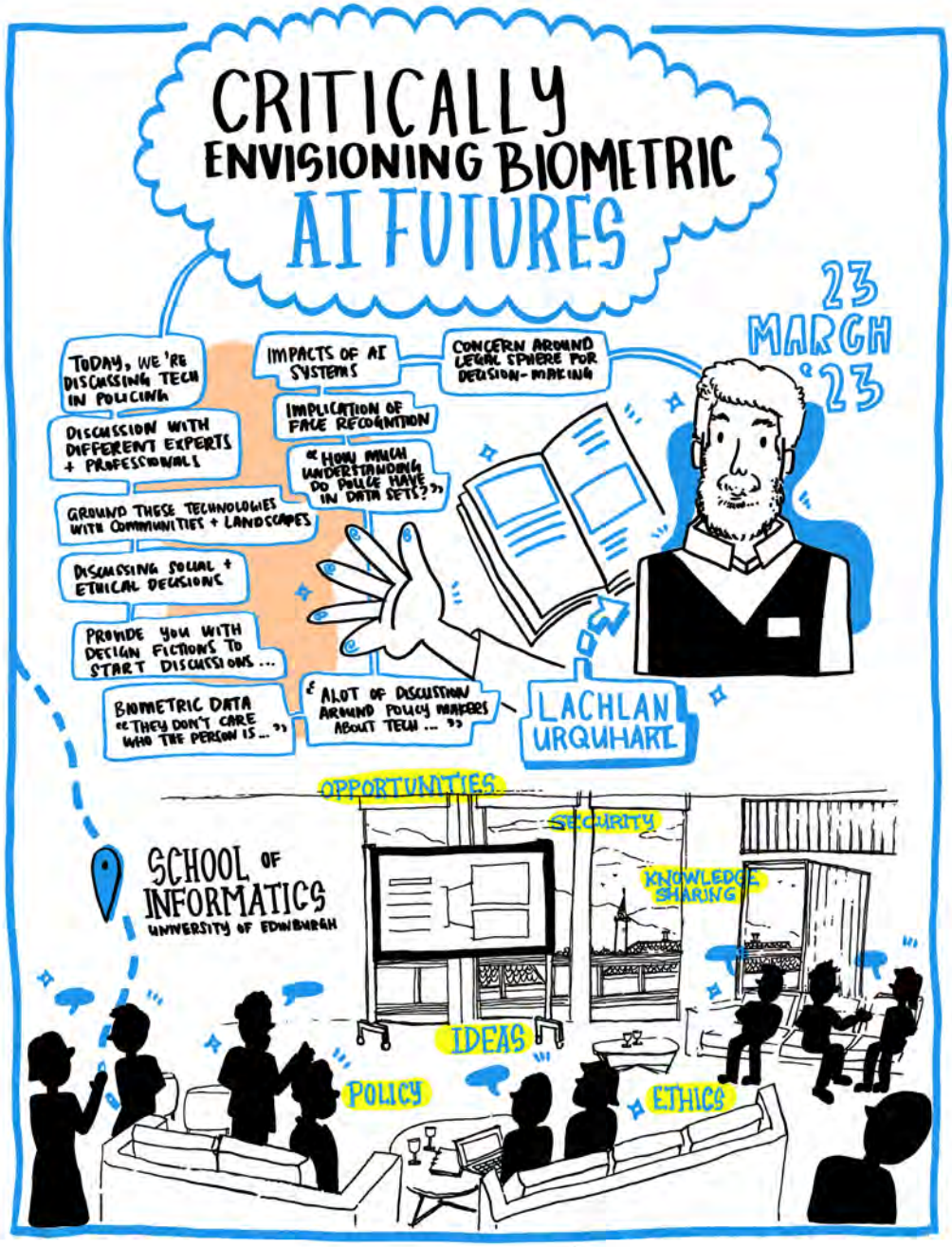
Of the six documents exploring the legal issues associated with DNA phenotyping technologies, one was based on interview and focus group data (Ahuriri-Driscoll 2021), while two were based on a review of case studies from the existing scholarly literature (Vajpayee and Shukla 2021; Murphy 2018). Three were based on an analysis of legal cases and the existing relevant case law (Albrecht 2020; Presser and Robertson 2021; Samuel and Prainsack 2018). The findings of the review for DNA phenotyping technologies are summarised in Table 3.

Table 3: Summary: DNA phenotyping technologies

Summary: DNA Phenotyping Technologies	
Number of Documents focusing on DNA Phenotyping Technologies (FDP) n=15	
Document Type	
Research Report	n=2
Conference Proceedings	n=1
Journal Article:	n=12
• Journals focusing on Social Impacts of Developments in Genetics and Bioscience	n=5
• Security Studies Journals	n=1
• Forensic Science Journals	n=4
• Criminology and Criminal Science Journals	n=2
Issues	
Social and Ethical Issues:	n=13
• Accuracy	n=8
• Bias and Discrimination	n=8
• Security	n=3
• Privacy	n=5
• Risk of Self Incrimination	n=1
• Ethical Questions over joint/collective responsibility	n=1
Suggestions to mitigate social and ethical challenges	
Evidence:	
• Existing literature	n=4
• Case study	n=3
• Interviews & focus groups	n=3
• Survey Data	n=2
• Laboratory Testing/Experiments	n=2
Legal Issues	
• Transparency and Fairness	n=3
• Retention of Personal Data	n=1
• 'Slippery Slope' Theory	n=1
• Legal Questions concerning the Right Not to Know	n=1
• Lack of Clarity over FDP in Existing Legal Frameworks	n=1
Suggestions/ to mitigate legal challenges	
Evidence:	
• Interviews and Focus Groups	n=1
• Existing Literature	n=2
• Legal Case Analysis	n=3

PART 4. STAKEHOLDER ROUNDTABLE

PART 4. STAKEHOLDER ROUNDTABLE



We hosted the High-Level Expert Roundtable in March 2023 with 15 attendees. This involved providing some background to the project and then presenting each of the three-design fictions live using Twine, with 40 minutes of group discussions afterwards and then final reflections to conclude. This roundtable was graphic recorded as seen below.

1. Key Discussion Points from the Roundtable

We will now consider a range of discussion points from the Roundtable. In terms of the method, there were numerous points of discussion. One queried how speculative should it be in terms of proximity to current operational approaches vs more futuristic representations of possibilities based on current stated of the art. There was interest in considering more explicit comparisons of the benefits and challenges of alternative approaches to the near future design fictions too e.g., sketch artists vs our AI system in scenario 3 or use of facial matching and mobile fingerprinting systems. Further, there was discussion that the method is valuable in bringing together different stakeholders to discuss these issues, and it could be used to elicit public perceptions too.

A. Live Automated Facial Recognition

Trustworthiness

The discussion was focused on the challenges policing will face in **managing public trust around new technologies**. Finding strategies for communicating how **technologies work to the public**

LIVE FACIAL RECOGNITION

CONSENT

WHAT DOES CONSENT MEAN IN THIS SCENARIO?

IT HAS AN IMPACT ON DEMOCRACY

"WOULD IT IMPACT PARTICIPATION IN PROTESTS?"

PRESUMPTION OF INNOCENCE

"POLICE HAVE SPECIFICALLY CHOSEN TO SURVEIL THIS SPACE ... POSES RISK ..."

IMPACT ASSESSMENT IN DIFFERENT FORMS ...

DIFFERENT LEVEL OF PRIVACY

"IN THIS SITUATION, YOU'RE UNLIKELY TO GAIN INFORMED CONSENT ..."

TRUST

HISTORIC RELATIONSHIP WITH POLICING BASED ON PUBLIC OPINION

"ARE WE ONLY LOOKING OUT FOR TERRORIST OR DOES IT INCLUDE EVERYONE?

PROPORTIONALITY

"WHAT DO YOU MEAN BY A WATCH LIST?"

PUBLIC TRUST TOWARDS INFO + TECH AFFECTS POLICING

PUBLIC TRUST + OPINION ON POLICING ...

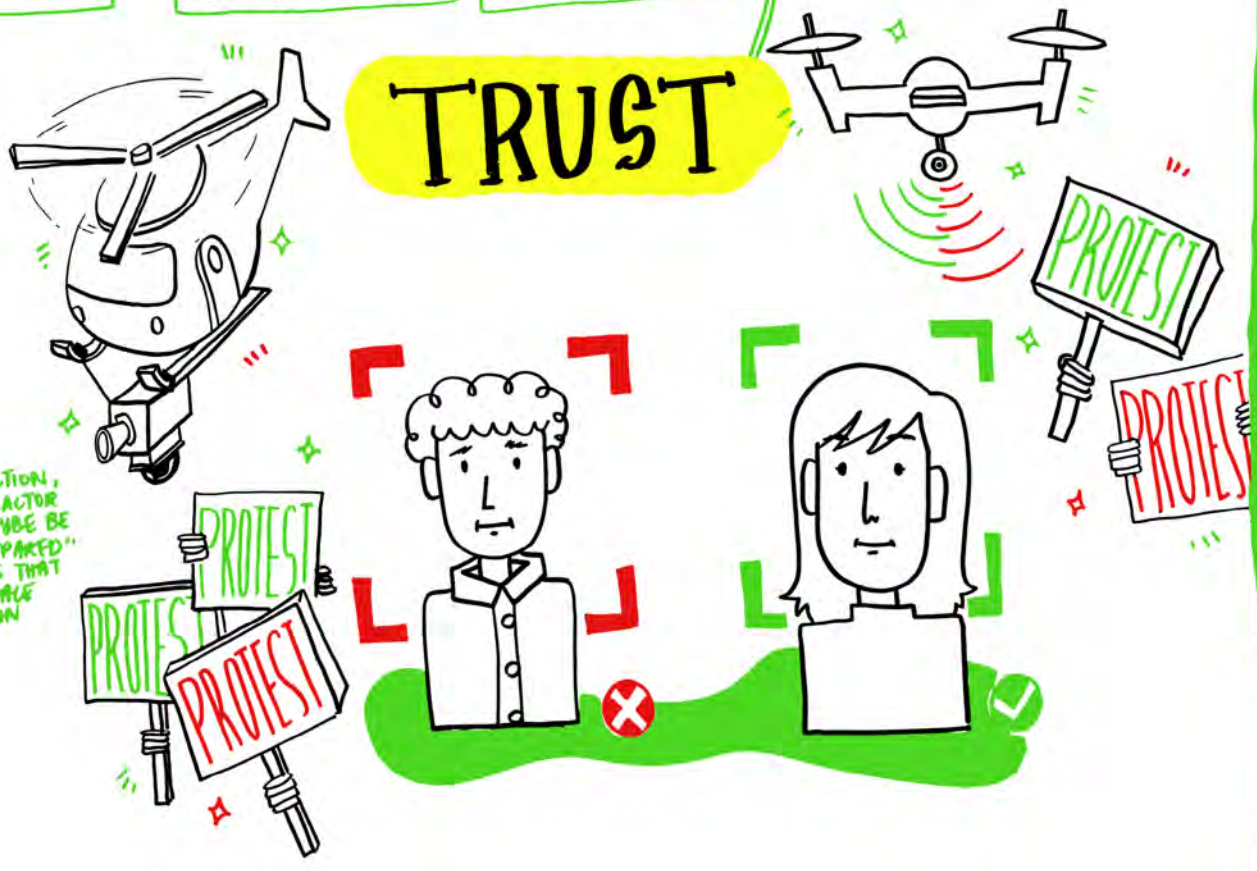
"MET POLICE HAS SOMETHING LIKE 13% PUBLIC TRUST..."

"PEOPLE HAVE A VERY SHORT TIME TO DECIDE WHETHER THEY TRUST THE TECH..."

SIGNS OF TRUSTWORTHINESS

DO PEOPLE EXPECT DATA TO BE USED THIS WAY?

"QUESTION AROUND POWER ... DO THE POLICE EVEN TRUST THE TECH + INFO?"



NOTE:
IN THE FICTION, PROTESTOR ACTOR SHOULD MAYBE BE "MORE PREPARED" IE. CLOTHES THAT COMBAT FACE RECOGNITION

so they can decide to trust usage or not, is one aspect. There is a challenge in managing the disconnect between public perceptions of what may be possible with police use of new technology, and the realities which are often less advanced e.g., volume of drone use by police is quite low.

Discussants noted trustworthiness requires attention to the technology, the institution, and even how police build trust in technology internally e.g., with **appropriate expertise** around data management. Further, demonstrating there are sufficient **safeguards and oversight mechanisms** prior to operation of technologies is important.

Oversight of Risks

There was debate about best mechanisms for providing oversight. **It was questioned if impact assessments (IAs)** are fit for purpose and capture enough information? Specifically, are Data Protection Impact Assessments too narrow, or can they capture the wider range of issues posed by LFR and similar technologies? In drafting IAs, the focus should not be on how long the documents are but the clarity in explaining and addressing fundamental risks and issues. There is value for a range of impact assessments focusing on human rights, data ethics, children's rights, and algorithmic.

Further, there was an awareness of the disconnect between what may be legal, and what is ethical, and how those distinctions feed into discussions around what is best practice and analysing of risks posed by technologies. Currently, it is felt there is not sufficient alignment in **how we evaluate risks from technology in terms of what the** public accepts, what is legally risky, and what are the ethical principles giding its use.

Data Protection Compliance

More broadly, data protection compliance remains central, particularly around storage and automated erasure of data, alongside addressing (in)accuracies with data used to identify citizens in situ. Further, there are fundamental questions around if such systems are **necessary, proportionate, lawful and fair**? With the latter two, consent is unlikely to be the lawful basis, and expectations of the public around fair use of their data needs to balance different rights, interests, and expectations. Technical questions around fitness for purpose of biometric data definitions and legal classifications also remain uncertain e.g., gait or thermal data as personal data?

Social Divisions

Formulating trustworthy relationships with the public cannot be a one size fits all approach, and there is scope for a digital divide if not addressed properly. Different lived experiences of citizens interacting with technologies may shape their trust or distrust in the police. This includes accounting for **vulnerable subjects of public space**, due to age, race, gender. Those who encounter the police more often may be more distrusting too. Thus, there are individual, community, and political dimensions shaping acceptance of new systems, which may shape tolerance of new systems.
When citizens are interacting with technologies in situ, better strategies to make sense of what the system does, and how different populations may accept or reject judgments form technology are needed. For example, with the face passport for consent giving in the fiction, not everyone at the event would have a phone, and thus may face different choices, or consequences as a result.

Formation of watchlists was one point requiring better strategies for communicating to the public who is on watchlists, and proportionality of them being there, e.g., those with warrants for arrest through to those at risk of causing significant harm (e.g., terrorism). The provenance of how data was sourced for watchlists was another concern, and there were concerns around impacts on **presumption of innocence** from being on a watchlist.

Data Ecology

The emerging data ecology around these systems was discussed, such as the power embedded in these technologies. Particularly, who operates the technology and who data will be shared with, for example data sharing across both public and private providers. For near future scenarios in the fiction, the type of support infrastructures necessary to facilitate these systems and data flows was questioned – how difficult would it be to allow cross device, system, and institutional sharing? This links into discussion around procurement, namely oversight for private companies around training datasets and models too.

Operational Value

More broadly, these systems posed questions about operational value, in terms of balancing benefits for police investigations and use of resources against costs to society. For example, without LFR the alternative is more manual processing, requiring more staff to look at CCTV. Yet, there is not enough officers, meaning the capacity/reality of budgets in policing may help make the case for LFR systems.

Societal Implications of Policing Protest

The scenario focused on policing public protest, leading to concerns around how these systems may have a chilling effect on exercising the right to assembly. How is this balanced against public safety? If too invasive, does this act as a deterrent to protest in future? How does this change resistance strategies and forensic awareness of citizens to resist technologies? Further, the use of drones in the scenario raised questions about their use. Currently there are operational restrictions of flying over protests where it is over everyone's head, not just protesters. This raises concerns around scope for privacy preserving processing in future. Further, drones can follow people around, creating new risks for privacy for mobile as opposed to traditional static surveillance.

B. Emotional AI

Accountability & Decision Making

There was interest in how the emotion monitoring systems interface with frontline officer practice. For example, how accountable were police officers for their actions if they act on what a system tells them? Does it lie with the system or them if a negative outcome occurs when they are interacting with the public? What happens with how the system captures actions of officers? Further discussion focused on the relationship between officer intuition and agency of officers using the system, where they are being guided to make decisions by the machine that goes against their instinct. Given experience of officers in reading situations and people, how will such systems account for that operational aspect of policing work? Will officer instinct be lost or eroded by such systems? Further, how might this manifest across generations in the force, between officers who have lots of experience working without the system and resist it or switch it off, vs newer officers who may adopt it more readily and rely on it? Or will there be ways to have human-AI interactions where it is not displacing or losing skills through the technology, but providing knowledge that is valuable to officers?

Operational Value

There was again discussion of to what extent AI could replace missing officers given budget constraints e.g., in this fiction, one officer was attending the scene instead of two. Despite concerns above, there was also discussion of positive uses. For example, could it provide new means of communication for frontline officers interacting with senior officers to provide guidance? Or could it help with wellbeing of officers to help monitor mental health and trauma to support them e.g., for example wellbeing of firearms officers during and after investigations for discharging weapons.

Nature of Emotion Recognition Systems

There were concerns about if Emotional Recognition technology works in practice, perceived as an immature technology. There were concerns if it is sufficiently accurate. This includes wider questions of if it is ethical (or legal) to deploy a system that may be convenient to use or serves a purpose but is inaccurate. This follows concerns around accuracy of other types of biometric systems such as gait recognition. Further, there was recognition that contexts of collection can impact accuracy where it is tested in lab type domains, yet policing operational situations may mean it does not work in those other domains for technical reasons. For example, how do emotion recognition systems account for voice, particularly dialects, tonality of voice and the cultural contingency of emotions and language. Has the system been tested cross-culturally? The lack of baseline for emotional stated, coupled with concerns around models of basic emotion underpinning these systems further posed questions about if they should be used. Biometrics are often framed as immutable (measuring of body e.g., DNA, fingerprints); but it was noted emotions are mutable, volatile and change. This also linked into more fundamental concerns around how to frame emotions and data, and impacts for governance with these systems. With the former, how do you codify human experience in data? How should it be measured? With the latter, is emotion data captured by data protection laws as biometric data when it is not focused

EMOTIONAL AI

IF POLICE WERE TO ACT BASED ON AI PROMPT, WHO TAKE ACCOUNTABILITY FOR ACTIONS?

"POLICE IS ALSO UNDER SURVEILLANCE"

YEARS OF EXPERIENCE IN UNDERSTANDING HUMAN EMOTION

IMBEDDING 'INTUITION' INTO TECH...

"JUST BECAUSE SOMETHING IS LEGAL, DOESN'T MEAN IT'S ETHICAL..."

IS IT ETHICAL TO DEPLOY SOMETHING WITH INACCURACIES? IT'S PREMATURE...

ACCOUNTABILITY

A QUESTION AROUND EMPATHY...

SKILLSETS OF AN OFFICER NEEDS TO EVOLVE WITH TIME... ALONGSIDE EVOLVING TECH

POLICE INSTINCTS + DECISION MAKING IN THE SITUATION

'CODIFYING' EXPERIENCE IN LAW ENFORCEMENT EG. EXPERIENCE AS A/WITH MINORITY + CHILDREN

HOW WOULD YOU 'CODIFY' HUMAN EMOTIONS?

HOW WOULD THIS BE WRITTEN IN ALGORITHMS?

EMOTIONAL DATA USED AS BIOMETRIC DATA

ACCURACY

WOULD IT BE A RELIABLE TOOL FOR REAL LIFE USE?

DE-VALUING HUMAN INTUITION

"IT COULD CAUSE MORE HARM IN THIS SITUATION"

WHAT IS THE BASELINE?

DIFFERENCES IN CULTURAL BACKGROUNDS, LANGUAGE + DIALECT, EMOTIONS...

"FROWN, SLIGHT SMILE, HEART RATE ETC..."

IMPACT ON VULNERABE PEOPLE EG. NEURODIVERGENT INDIVIDUALS

THOSE WHO PERCEIVE EMOTIONS DIFFERENTLY

DE-ESCALATE

on identification? Can you consent to this data being processed?

Community Trust and Cultural Dimensions

Beyond concerns around the technology itself, there was discussion about ensuring that systems were not just about enhancing public safety but public good and focusing on its role for good as a measure to justify its use. Again, the question was how best to explain to communities meeting the criminal justice system more regularly, what these systems are doing? Or how to ensure issues for vulnerabilities of certain groups at risk of harmful assumptions are not being built into these technologies e.g., neurodiversity, racial bias. Given scope for disproportionately more harmful consequences, what does it mean for all being treated equally and fairly by the systems? Are there ways to involve professionals who work with vulnerable groups in policing strategy using roll-out of technologies that may impact groups with protected characteristics?

C. DNA Phenotyping

Safeguards and Potential Future Advancements

.

Given advances in DNA analysis and phenotyping systems, there was discussion of how to treat this class of data differently. For example, to support use of DNA phenotyping, there may be desire to keep DNA profiles and biological samples for longer periods of time. In practice though, the retention periods differ depending on seriousness of offence (it can be long for violent crimes) but there remains a need to justify the purposes of retention. Thus, whilst there may be value in keeping data for new methods of analysis that are emerging, questions remain about how oversight might adapt to new technological capabilities and address long term data management issues e.g., managing data of the deceased. Considering issues from greater interaction between digital forensics with growth of digital phenotyping would be important too – e.g., tracking of other behavioural characteristics through devices like wearables in investigations.

Identity

There was discussion around how DNA phenotyping may entrench certain aspects of identity by genetically defining who people are through biogeographical information and physical characteristics (such as skin, hair, and eye colour), shaping how populations are defined. There remains need for scope to be able to question those identities in relation to our bodies, but these systems can prevent that.

Legal Oversight of Commercial DNA Services

There were concerns around the interactions between public and private sector in supporting DNA phenotyping. For example, data might not be available through police sources and national databases – so alternatives might be needed, such as commercial genealogical services. However, there are differences between how police and private sector are regulated in collection and use of DNA. Thus, any private sector cooperation with law enforcement would need to be subject to adequate legal oversight in future. This includes around ensuring compliance with data protection in private suppliers, alongside complications of international data sharing across borders, which may require new UK primary legislation.

DNA PHENOTYPE

IDENTITY

- WOULD IT EMBED BIASES EG. RACE + STEREOTYPES?
- REPRESENTATION OF EVOLUTION OF TECHNOLOGY
- AGAIN... WHERE IS THE BASE LINE?
- COMPARISONS CAN BE PART OF THE DISCUSSION...
- PROBLEMATIC USING DNA TO SEARCH TO POPULATION
- NOT ENOUGH LEGISLATION
- COMMERCIAL SUPPLIERS OF DNA - ANCESTRY
- LEGAL OVERSIGHT?
- INTERNATIONAL DIMENSIONS WILL AFFECT THIS.. UK CAN'T SHARE THIS DATA
- REPURPOSING OF DATA.. PRIVATE ENTITIES OWNING DATA - GDPR
- POLICE + LAW ENFORCEMENT CAN REPURPOSE DATA
- DATA IS SAFEGUARDED DUE TO SENSITIVITIES
- AUTHORIZED BY LAW...

RELIABILITY

- FORENSIC SCIENCE WILL USE THIS TECH TO SOLVE CASES THAT WERE UNSOLVED FOR YEARS...
- IT'S A TECHNIQUE THAT'S BEING USED NOW!
- DNA IS SENSITIVE INFORMATION... IT'S PROTECTED BY DATA ACT...
- "IS THERE PRESSURE TO RETAIN SAMPLES FOR AS LONG AS POSSIBLE...?"
- "AT WHAT POINT DOES DNA DETERIORATE?"
- "THE SCIENCE PROBABLY HAS CAUGHT UP...?"
- "YOU CAN KEEP SAMPLE FOR AS LONG AS YOU WANT BASED ON LAW..."
- HOW DO WE ASSESS RISK?
- DIGITAL PHENOTYPE TO CONTRIBUTE TO UNDERSTAND WELL-BEING + BEHAVIOUR
- DIGITAL BIOMETRIC DATA

PART 5. FINAL REFLECTIONS

The Design Fictions provided a valuable method to speculate and envision how technologies might be used in the near future and reflect on societal impacts. Our fictions were narrative based, and mixed utopian and dystopian components, showcasing the contested nature of Biometric AI in different contexts. The fictions were both a provocative and discursive tool to help us think about futures we want to create or avoid, providing means to reflect on the opportunities and challenges of Biometric AI in a creative way.

These fictions also supported discussion of complex issues; allowing us to situate emerging uses of technology and to reflect on a wide variety of social, ethical, and legal concerns. Common to all scenarios, the participants raised questions around fitness for purpose of a range of regulatory frameworks and oversight (namely how technologies challenge scope and application of laws). Another key discussion point was the importance of considering and understanding the needs of the public in relation to these systems in terms of design and operational roll out, particularly when engaging with diverse and vulnerable populations. The potential operational value of these biometric systems was also emphasised, while reflecting on how they might impact and challenge policing practice and oversight. Lastly, another key discussion point that emerged in all scenarios was the divergence of the promise and reality of these technological systems, namely in relation to issues of accuracy.

Some of these concerns were in line with a range of social, ethical, and legal issues explored in the literature reviewed. The systematic review demonstrated there were concerns common to all three types of biometric AI technologies, namely: accuracy, potential for bias and discrimination (including racial and ethnic bias), privacy, and security of sensitive, biometric data. Issues concerning a lack of regulation and ethical guidelines, trust, legitimacy of use, increased surveillance, consent for data capture and concerns over access control of data stored were also raised.

The short project highlighted the value of creative design methods for exploring complex social, ethical and legal aspects of biometric AI in law enforcement. There is scope for further novel research to build on findings and insights documented in this report.

PART 6. REFERENCES

- Abdulrahman, S. A., and Alhayani, B. (2023) A comprehensive survey on the biometric systems based on physiological and behavioural characteristics. Materials Today: Proceedings, 80: 2642-2646. DOI: 10.1016/j.matpr.2021.07.005
- Ada Lovelace Institute (2019). Beyond face value: public attitudes to facial recognition technology. Published by the Ada Lovelace Institute: London. Available at https://www.adalovelaceinstitute.org/report/beyond-face-value-public-attitudes-to-facial-recognition-technology/
- Ahuriri-Driscoll, A., Tauri, J., and Veth, J. (2021) Māori views of forensic DNA evidence: an instrument of justice or criminalizing technology? New Genetics and Society, 40:3, 249-266, DOI: 10.1080/14636778.2020.1829463
- Aizenberg, E., and van den Hoven, J. (2020). Designing for Human Rights in AI. Big Data and Society, 7, 2. https://doi.org/10.1177/2053951720949566
- Albrecht, H-J. (2020) Data, Data Banks and Security, European Journal for Security Research, 5:5–23, https://doi.org/10.1007/s41125-019-00062-9
- Alikhademi, K., Drobina, E., Prioleau, D., Richardson, B., Purves, D., and Gilbert, J. E. (2021). A review of predictive policing from the perspective of fairness. Artificial Intelligence and Law, 30 (1):1-17. DOI: 10.1007/s10506-021-09286-4
- Almeida, D., Shmarko, K., and Lomas, E. (2022). The ethics of facial recognition technologies, surveillance, and accountability in an age of artificial intelligence: a comparative analysis of US, EU, and UK regulatory frameworks. AI Ethics, 2: 377–387. https://doi.org/10.1007/s43681-021-00077-w
- Andalibi, N., and Buss, J. (2020). The Human in Emotion Recognition on Social Media: Attitudes, Outcomes, Risks. Proceedings of the ACM SIGCHI Conference on Human Factors in Computing Systems (CHI) 2020. DOI:10.1145/3313831.3376680
- Asaro, P. M. (2019). AI Ethics in Predictive Policing. From Models of Threat to an Ethics of Care. IEEE Technology and Society Magazine, 40-52. DOI: 10.1109/MTS.2019.2915154
- Atwood, L., Raymond, J., Sears, A., Bell, M., and Daniel, R. (2021) From Identification to Intelligence: An Assessment of the Suitability of Forensic DNA Phenotyping Service Providers for Use in Australian Law Enforcement Casework. Frontiers in Genetics, 11: 568701. DOI: 10.3389/fgene.2020.568701
- Babuta, A., and Oswald, M., (2020) Data Analytics and Algorithms in Policing in England and Wales: Towards A New Policy Framework, Royal United Services Institute for Defence and Security Studies
- Bargenda, J.A., & Wilson-Stark, S. (2018). The legal Holy Grail? German lessons on codification for a fragmented Britain. Edinburgh Law Review, 22(2) 183-210
- Barkane, I. (2022). Questioning the EU proposal for an Artificial Intelligence Act: The need for prohibitions and a stricter approach to biometric surveillance. Information Polity, 27: 147–162. DOI 10.3233/IP-211524
- Barrett, D., & Heale, R. (2020). What are Delphi Studies? Evidence-based nursing, 23(3), 68–69. https://doi.org/10.1136/ebnurs-2020-103303
- Becerra-Riera, F., Morales'Gonzalez, A., and Mendez-Vazquez, H. (2019). A survey on facial soft biometrics for video surveillance and forensic applications, Artificial Intelligence Review, 52(2): 1155-1187. https://doi.org/10.1007/s10462-019-09689-5
- Beck, R. A., (2021). Artificial Intelligence, Predictive Policing, and Risk Assessment for Law Enforcement, Annual Review of Criminology, 4(1): 209-237
- Bleecker, J. (2009) "Design Fiction: A Short Essay on Design, Science, Fact and Fiction." California: Near Future Laboratory. http://blog.nearfuturelaboratory.com/2009/03/17/ design-fiction-a-short-essay-on-design-science-fact-and-fiction/.
- Benjamin, R (2019) Race After Technology. Polity Press: Medford.
- Bosch, T. (2012) "Sci-Fi Writer Bruce Sterling Arguedd the Intriguing New Concept of Design Fiction." Slate. https://slate.com/technology/2012/03/bruce-sterling-on-design-fictions.html
- Bradford, B., Yesberg, J. A., Jackson, J., and Dawson, P., (2020). Live Facial Recognition: Trust and Legitimacy as Predictors of Public Support For Police Use of New Technology, The British Journal of Criminology, 60, 6, 1502–1522, https://doi.org/10.1093/bjc/azaa032
- Bragias, A., Hine, K., & Fleet, R., (2021) 'Only in our best interest, right?' Public perceptions of police use of facial recognition technology, Police Practice and Research, 22, 6, 1637-1654, DOI: 10.1080/15614263.2021.1942873
- Brey, P. (2012). Anticipating Ethical Issues in Emerging IT. Ethics and Information Technology, 14, 4: 305–317

- Brey, P. (2017). Ethics of Emerging Technologies. In S. O. Hansson (Ed.), Methods for the Ethics of Technology. Rowman and Littlefield International.
- Bromberg, D. E., Charbonneau, E., & Smith, A. (2020). Public support for facial recognition via police body-worn cameras: Findings from a list experiment, Government Information Quarterly, 37, 1, https://doi.org/10.1016/j.giq.2019.101415.
- Bryman, A. (2012). Social Research Methods (4th edition), Oxford University Press, United States
- Chowdhury, A. I., Shahriar, M. M., Islam, A., Ahmed, E., Karim, A., and Islam, M. R. (2020). An Automated System in ATM Booth Using Face Encoding and Emotion Recognition Process. IPMV '20: Proceedings of the 2020 2nd International Conference on Image Processing and Machine Vision. 57-62. https://doi.org/10.1145/3421558.3421567
- Claypoole, T. (2021) Warrants Needed for Biometric Analysis, 65 St. Louis U. L.J. Available at: https://scholarship.law.slu.edu/lj/vol65/iss4/8 (Accessed 27th April 2023).
- College of Policing (2021) Police Use of Live Facial Recognition. https://www.college.police.uk/article/police-use-live-facial-recognition-technology-have-your-say>
- Colman, R. (2021). Police Facial Recognition in Progress: The Construction of the Notion of Accuracy in the Live Facial Recognition Technology Used by the MET Police in London. London School of Economics and Political Science: London.
- Connon, I. L. C., Egan, M., Hamilton-Smith N., Mackay, N., Miranda, D., and Webster, C. W. R. (2023) Review of emerging technologies in policing: Findings and recommendations. Scottish Government: Edinburgh. ISBN 9781805253518. Available at: https://www.gov.scot/publications/review-emerging-technologies-policing-findings-recommendations/ (Accessed 20th April 2023).
- Dechesne, F., Dignum, V., Zardiashvili, L., and Bieger, J. (2019). AI & Ethics at the Police: Towards Responsible use of Artificial Intelligence in the Dutch Police. Leiden/ Delft: Universiteit Leiden.
- Douglas, S., and Welsh, B. C., (2022) There has to be a better way: place managers for crime prevention in a surveillance society, International Journal of Comparative and Applied Criminal Justice, 46(1): 67-80, DOI: 10.1080/01924036.2020.1788960
- Dudhwala, F. (2020). Facial recognition technology: A guide for the dazed and confused. Centre for Data Ethics and Innovation Blog: Published online. Available at: https://cdei.blog.gov.uk/2020/06/01/facial-recognition-technology-a-guide-for-the-dazed-and-confused/ (Accessed 6th March 2023).
- Dworzecki, J., and Nowicka, I. (2021). Artificial Intelligence (AI) and ICT-Enhanced Solutions in the Activities of Police Formations in Poland. DOI - 10.1007/978-3-030-88972-2_11.
- Ellison, M., Bannister, J., Lee, W. D., & Haleem, M. S. (2021). Understanding policing demand and deployment through the lens of the city and with the application of big data. Urban Studies, 58, 15, 3157–3175. https://doi.org/10.1177/0042098020981007
- Eneman, M., Ljungberg, J., Raviola, E., and Rolandsson, B. (2022). The sensitive nature of facial recognition: Tensions between the Swedish police and regulatory authorities. Information Polity, 27: 219–232. DOI 10.3233/IP-211538
- Ernst, S., Veen, H., and Kop, N. (2021). Technological innovation in a police organization: Lessons learned from the National Police of the Netherlands, Policing: A Journal of Policy and Practice, 15, 3: 1818–1831, https://doi.org/10.1093/police/paab003
- Faraldo Cabana, P. (2023). Technical and Legal Challenges of the Use of Automated Facial Recognition Technologies for Law Enforcement and Forensic Purposes. In: Završnik, A., Simončič, K. (eds) Artificial Intelligence, Social Harms and Human Rights. Critical Criminological Perspectives. Palgrave Macmillan, Cham. https://doi.org/10.1007/978-3-031-19149-7_2
- Fontes, C., and Perrone, C. (2021). Ethics of surveillance: harnessing the use of live facial recognition technologies in public spaces for law enforcement. Institute for Ethics in Artificial Intelligence: Munich.
- Fontes, C., Huhma, E., Corrigan, C. C., and Lutge, C. (2022). AI-powered public surveillance systems: why we (might) need them and how we want them. Technology in Society, 71: 102137, https://doi.org/10.1016/j.techsoc.2022.102137.
- Fussey, P. Davies, B., & Innes, M. (2021), 'Assisted' facial recognition and the reinvention of suspicion and discretion in digital policing, The British Journal of Criminology, 61, 2, 325–344, https://doi.org/10.1093/bjc/azaa068
- Fussey, P., and Murray, D. (2019), Independent Report on the London Metropolitan Police Service's Trial of Live Facial Recognition Technology, University of Essex Human Rights, http://repository.essex.

PART 6. REFERENCES

- Grimond, W., and Singh, A., (2020), A Force for Good: Results from FOI requests on artificial intelligence in the police force. Royal Society for the encouragement of Arts, Manufactures and Commerce. https://www.thersa.org/globalassets/reports/2020/aforce-for-good-police-ai.pdf
- Davis, K. and Harriss, L. (2018) Biometric Technologies. Technical report. Parliamentary Office of Science and Technology. Available at: https://post.parliament.uk/research-briefings/post-pn-0578/
- Guo, Z., and Kennedy, L. (2023). Policing based on automatic facial recognition. Artificial Intelligence and Law 31 (2):397-443.
- Harris, E., Khoo, I-H., and Demircan, E. (2022) A Survey of Human Gait-Based Artificial Intelligence Applications. Frontiers in Robotics and Artificial Intelligence, 8:749274. DOI: 10.3389/frobt.2021.749274.
- Hayward, K. J., & Maas, M. M. (2021). Artificial intelligence and crime: A primer for criminologists. Crime, Media, Culture, 17, 2, 209–233. https://doi.org/10.1177/1741659020917434
- Hill, D., O'Connor, C. D., and Slane, A. (2022). Police use of facial recognition technology: The potential for engaging the public through co-constructed policy-making. International Journal of Police Science & Management, 24(3): 325–335. https://doi.org/10.1177/14613557221089558
- Hobson, Z., Yesberg, J.A., Bradford, B. et al. (2021), Artificial fairness? Trust in algorithmic police decision-making. J Exp Criminol. https://doi.org/10.1007/s11292-021-09484-9
- Hood, J., (2020), Making the Body Electric: The Politics of Body-Worn Cameras and Facial Recognition in the United States, Surveillance and Society, 18, 2, 157-169
- Hopman, R. (2020) Opening up forensic DNA phenotyping: the logics of accuracy, commonality and valuing, New Genetics and Society, 39:4, 424-440, DOI: 10.1080/14636778.2020.1755638
- Information Commissioner's Office (2021). Information Commissioner's Opinion: The use of live facial recognition technology in public places. ICO Information Commissioner's Office. Available at: https://ico.org.uk/media/2619985/ico-opinion-the-use-of-lfr-in-public-places-20210618.pdf (Accessed 4th April 2023).
- Information Commissioner's Office (2022). Biometric: Foresight. https://ico.org.uk/media/4021971/biometrics-foresight-report.pdf
- Information Commissioner's Office (2023) Guidance on AI and data protection. https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/artificial-intelligence/guidance-on-ai-and-data-protection/
- Jansen, F., Sánchez-Monedero, J., and Dencik, L. (2021). Biometric identity systems in law enforcement and the politics of (voice) recognition: The case of SiiP. Big Data and Society, 8, 2: 1-13. DOI: 10.11 7 7/20 539517211063604
- Jensen, T., and Vistisen, P. (2017) Ethical Design Fiction: Between Storytelling and World Building. The Orbit Journal 1(2): 1–4. https://doi.org/10.29297/orbit.v1i2.56.
- Jupe, L. M., and Keatley, D. A. (2020). Airport artifcial intelligence can detect deception: or am I lying? Security Journal, 33:622–635. https://doi.org/10.1057/s41284-019-00204-7
- Katsara, M-A., Branicki, W., Po'spiech, E., Hysi, P., Walsh, S., Kayserf, M., and Nothnagel, M. (2021), Testing the impact of trait prevalence priors in Bayesian-based genetic prediction modeling of human appearance traits. Forensic Science International: Genetics, 50: 102412. DOI: 10.1016/j.fsigen.2020.102412
- Keenan, B. (2021), Automatic Facial Recognition and the Intensification of Police Surveillance. The Modern Law Review, 84: 886-897. https://doi.org/10.1111/1468-2230.12623
- Kostka, G., Steinacker, L., and Meckel, M. (2023). Under big brother's watchful eye: Cross-country attitudes toward facial recognition technology, Government Information Quarterly, 40(1): 101761, https://doi.org/10.1016/j.giq.2022.101761
- Kulka-Bartoszek, M., Pośpiech, E., Woźniak, A., Boroń., M., Karlowska-Pik, J., Teissevre, P., Zubańska., M., Bronikowska, A., Grzybowski, T., Ploski, R., Spólnicka., M., and Branicki, W. (2019) DNA-based predictive models for the presence of freckles. Forensic Science International: Genetics, 42: 252-259. DOI: 10.1016/j.fsigen.2019.07.012
- Laffer, A (2022) Using an online narrative approach to explore diverse participants' understanding of emerging technology: Citizen's perspectives on living with emotional AI in SAGE Research Methods: Doing Research Online. London: Sage. https://doi.org/10.4135/9781529604122
- Leslie, D. (2019). Understanding artificial intelligence ethics and safety: A guide for the responsible design and implementation of AI systems in the public sector. The Alan Turing Institute. https://doi.org/10.5281/zenodo.3240529
- Machado, H., and Silva, S. (2019) What influences public views on forensic DNA testing in the criminal field? A scoping review of quantitative evidence. Human Genomics, 13:23, https://doi.org/10.1186/s40246-

019-0207-5
- Markussen, T., and Knutz, E. (2013). The Poetics of Design Fiction. In Proceedings of the 6th International Conference on Designing Pleasurable Products and Interfaces. DPPI '13, University of Northumbria, UK, 231–40. New York: Association for Computing Machinery https://dl.acm.org/doi/abs/10.1145/2513506.2513531.
- McGuire, M. R. (2021) The laughing policebot: automation and the end of policing, Policing and Society, 31, 1, 20-36, DOI: 10.1080/10439463.2020.1810249
- McKendrick, K. (2019). Artificial Intelligence Prediction and Counterterrorism. The Royal Institute of International Affairs, Chatham House: London. Available at: https://www.chathamhouse.org/sites/default/files/2019-08-07-AICounterterrorism.pdf (Accessed 18th April 2023).
- McStay, A., and Urquhart, L. (2019) 'This time with feeling?' Assessing EU data governance implications of out of home appraisal based emotional AI, first Monday, 24, 10-7.
- McStay, A. (2018) Emotional AI: The Rise of Empathic Media. SAGE
- Miller, S., and Smith, M. (2022) Quasi-Universal Forensic DNA Databases. Criminal Justice Ethics, 41:3, 238-256, DOI: 10.1080/0731129X.2022.2141021
- Mohamed, S., Png, M-T., and Isaac, W. (2020). Decolonial AI: Decolonial Theory as Sociotechnical Foresight in Artificial Intelligence. Philosophy & Technology, 33:659–684. https://doi.org/10.1007/s13347-020-00405-8
- Moses, L.B. (2013) How to Think about Law, Regulation and Technology: Problems with 'Technology' as a Regulatory Target, Law, Innovation and Technology, 5:1, 1-20, DOI: 10.5235/17579961.5.1.1
- Murphy, E. (2018). Forensic DNA Typing. Annual Review of Criminology, 1: 497-515. https://doi.org/10.1146/annurev-criminol-032317-092127
- Nkonde, M. (2020). Automated Anti-Blackness: Facial Recognition in Brooklyn, New York. Harvard Kennedy School Journal of African American Policy, 2019-2020 edition: 30-37.
- Noriega, M., (2020) The application of artificial intelligence in police interrogations: An analysis addressing the proposed effect AI has on racial and gender bias, cooperation, and false confessions, Futures, 117, 102510, https://doi.org/10.1016/j.futures.2019.102510.
- Oswald, M. (2022), A three-pillar approach to achieving trustworthy and accountable use of AI and emerging technology in policing in England and Wales: Lessons from the West Midlands data ethics model, European Journal of Law and Technology, 13, 1: https://ejlt.org/index.php/ejlt/article/view/883/1045
- Pal, S., Mukhopadhyay, S., and Suryadevara, N. (2021). Development and Progress in Sensors and Technologies for Human Emotion Recognition. Sensors, 21: 5554. https://doi.org/10.3390/s21165554
- Pauwels, E. (2020). Artificial Intelligence and Data Capture Technologies in Violence and Conflict Prevention Opportunities and Challenges for the International Community. Global Center on Cooperative Security: Washington. Available at: https://www.globalcenter.org/resource/artificial-intelligence-and-data-capture-technologies-in-violence-and-conflict-prevention/ (Accessed 10th April 2023).
- Podoletz, L. (2021). We have to talk about emotional AI and crime. AI and Society, 38: 1067–1082. https://doi.org/10.1007/s00146-022-01435-w
- Presser, J. R., and Robertson, K. (2021). AI Case Study: Probabilistic Genotyping DNA Tools in Canadian Criminal Courts. Law Commission of Ontario: Toronto. Available at https://www.lco-cdo.org/en/our-current-projects/ai-adm-and-the-justice-system/ai-case-study-pg/ (Accessed 25 April 2023).
- Purshouse, J., and Campbell, L. (2022). Automated facial recognition and policing: a Bridge too far? Legal Studies, 42, 209–227, doi:10.1017/lst.2021.22
- Queirós, F. (2019). The visibilities and invisibilities of race entangled with forensic DNA phenotyping technology. Journal of Forensic and Legal Medicine, 68: 101858. https://doi.org/10.1016/j.jflm.2019.08.002
- Raposo, V. L. (2022). The Use of Facial Recognition Technology by Law Enforcement in Europe: a Non-Orwellian Draft Proposal. Eur J Crim Policy Res. https://doi.org/10.1007/s10610-022-09512-y
- Ryder, M. (2022). The Ryder Review: Independent legal review of the governance of biometric data in England and Wales. Ada Lovelace Institute. ISBN: 978-1-7397950-1-6. Available at:
- https://www.adalovelaceinstitute.org/report/ryder-review-biometrics (Accessed 27th February 2023).
- Samuel, G., and Prainsack, B. (2018). The regulatory landscape of forensic DNA phenotyping in Europe. VISAGE Visible Attributes through Genomics: London. Available at: https://www.visage-h2020.eu/PDF/Deliverable_5.1_for_posting_online_DECEMBER_2018.pdf (Accessed 21st April 2023).
- Samuel, G., and Prainsack, B. (2019) Forensic DNA phenotyping in Europe: views "on the ground" from those who have a professional stake in the technology, New Genetics and Society, 38:2, 119-141, DOI: 10.1080/14636778.2018.1549984

PART 6. REFERENCES

- Sandelowski, M. (2000) Whatever happened to qualitative description? Res Nurs Health, 23(4):334-340. doi:10.1002/1098-240x(200008)23:4<334::aid-nur9>3.0.co;2-g
- Sarabdeen, J. (2022). Protection of the rights of the individual when using facial recognition technology. Heliyon, 8(3): e09086. DOI:10.1016/j.heliyon.2022.e09086
- Scottish Biometrics Commissioner (2022) Code of Practice. https://www.biometricscommissioner.scot/media/cnxb3ncn/biometrics-code-of-practice-draft-to-be-laid.pdf
- Scudder, N., Robertson, J., Kelty, S. F., Walsh, S. J., and McNevin, D. (2019). A law enforcement intelligence framework for use in predictive DNA phenotyping, Australian Journal of Forensic Sciences, 51:sup1, S255-S258, DOI: 10.1080/00450618.2019.1569132
- Smith, M., & Miller, S. (2022), The ethical application of biometric facial recognition technology. AI & Society, 37: 167–175 https://doi.org/10.1007/s00146-021-01199-9
- Snilstveit, B., Oliver, S. & Vojtkova, M. (2012). Narrative approaches to systematic review and synthesis of evidence for international development policy and practice, Journal of Development Effectiveness, 4(3), 409-29. https://doi.org/10.1080/19439342.2012.710641
- Sollie, P. (2007). Ethics, Technology Development and Uncertainty: An Outline for any Future Ethics of Technology. Journal of Information, Communications & Ethics in Society, 5(4): 293–306
- Stahl, B. C., Timmermans, J., and Flick, C., (2017), Ethics of Emerging Information and Communication Technologies: On the implementation of responsible research and innovation, Science and Public Policy, 44(3): 369–381, https://doi.org/10.1093/scipol/scw069
- Sterling, B. (2013) "Patently Untrue: Fleshy Defibrillators and Synchronised Baseball Are Changing the Future." Wired UK. https://www.wired.co.uk/article/patently-untrue.
- Urquhart, L., and Miranda, D. (2022) Policing faces: the present and future of intelligent facial surveillance, Information & Communications Technology Law, 31:2, 194-219, DOI: 10.1080/13600834.2021.1994220
- Urquhart, L., McGarry, G., and Crabtree, A. (2022) Legal provocations for HCI in the design and development of trustworthy autonomous systems. Proceedings of the 12th Nordic Conference on Human-Computer Interaction (NordiCHI'22): Aarhus, Denmark 8th – 12th October, 2022. ACM, p. 1-12 12 p. 75.
- Urquhart, L., Miranda, D. and Laffer, A. (2022) Working with Affective Computing: Exploring UK Public Perceptions of AI enabled Workplace Surveillance. In: Effectiveness of ICT ethics – How do we help solve ethical problems in the field of ICT?. ETHICOMP 2022, University of Turku, Finland, 165-177. https://sites.utu.fi/ethicomp2022/proceeding/
- Vajpayee, K., and Shukla, R. K. (2021). DNA Phenotyping: The Technique of the Future. In: Dash, H. R., Shrivastava, P., Lorente, J. A. (eds) Handbook of DNA Profiling. Springer: Singapore. https://doi.org/10.1007/978-981-15-9364-2_54-1
- Webster, W., Miranda, D. and Leleux, C. (2022) Evidence Review into Public Experience and Confidence of Body Worn Video in a Policing Context. University of Stirling. http://hdl.handle.net/1893/34460
- Whittlestone, J. Nyrup, R. Alexandrova, A. Dihal, K. and Cave, S. (2019) Ethical and societal implications of algorithms, data, and artificial intelligence: a roadmap for research. Nuffield Foundation: London.
- Williams, D. P. (2020), Fitting the description: historical and sociotechnical elements of facial recognition and anti-black surveillance. Journal of Responsible Innovation, 7, supplement 1, 74-83. DOI: 10.1080/23299460.2020.1831365
- Wright, J. (2021). Suspect AI: Vibraimage, Emotion Recognition Technology and Algorithmic Opacity. Science, Technology & Society, 1-20 https://doi.org/10.1177/0971721821100341
- Wright, D., and Friedewald, M., (2013), Integrating privacy and ethical impact assessments, Science and Public Policy, 40, 6: 755–766, https://doi.org/10.1093/scipol/sct083

PART 7. APPENDICES

Table 1 - Review of Biometric AI Technologies in Policing: Summary of Findings

Number of Documents focusing on DNA Phenotyping Technologies (FDP) n=15

	Total Number of Documents in the Sample N=77				
	Behaviour and Emotion Detection Artificial Intelligence Technologies n=14				Live Facial Recognition Technologies n=51
	Voice	Gait	Body language	Writing	
Social and Ethical Issues:	n=7	n=1	n=5	n=1	n=32
• Accuracy	n=3	n=1	n=2	n=1	n=11
• Bias and discrimination	n=4	n=0	n=0	n=0	n=18
• Dependency	n=1	n=0	n=0	n=0	n=0
• Privacy, freedom	n=5	n=0	n=1	n=1	n=18
• Lack of regulation	n=2	n=0	n=1	n=0	n=9
• Legitimacy	n=0	n=1	n=1	n=0	n=14
• Surveillance	n=0	n=1	n=0	n=0	n-6
• Security	n=0	n=0	n=1	n=0	n=7
• Trust	n=0	n=0	n=1	n=0	n=12
• Consent	n=0	n=0	n=0	n=0	n=6
• Access control	n=0	n=0	n=0	n=0	n=8
• Biodeterministic criminalisation	n=0	n=0	n=0	n=0	n=1
• Risk of self-incrimination	n=0	n=0	n=0	n=0	n=0
• Collective responsibility	n=0	n=0	n=0	n=0	n=0
Evidence base:					
• Existing literature	n=6	n=1	n=2	n=1	n=17
• Case study	n=1	n=0	n=0	n=0	n=9
• Historical documents	n=0	n=0	n=1	n=0	n=0
• Survey data	n=0	n=0	n=1	n=0	n=3
• Legal document analysis	n=0	n=0	n=1	n=0	n=2
• Interviews & focus groups	n=0	n=0	n=1	n=0	n=1
• Laboratory testing/experiments	n=0	n=0	n=0	n=0	n=0
Suggestions & recommendations: Mitigating social & ethical issues	n=2	n=0	n=1	n=1	n=14
Legal Issues	n=0	n=0	n=3	n=0	n=11
• Human Rights and equality	n=0	n=0	n=1	n=0	n=11
• Weakening of rule of law	n=0	n=0	n=2	n=0	n=0
• Limitations of existing legal frameworks	n=0	n=0	n=1	n=0	n=1
• Data Protection	n=0	n=0	n=0	n=0	n=8
• Necessity & proportionality	n=0	n=0	n=0	n=0	n=1
• Choice	n=0	n=0	n=0	n=0	n=1
• Watchlist Generation	n=0	n=0	n=0	n=0	n=1
• Protection of Children	n=0	n=0	n=0	n=0	n=1
• Potential of EU AI Regulations	n=0	n=0	n=0	n=0	n=1
• Challenges to Criminal Procedure Act	n=0	n=0	n=2	n=0	n=1
• Transparency & Fairness	n=0	n=0	n=0	n=0	n=0
• The right not to know	n=0	n=0	n=0	n=0	n=0
Evidence base:					
• Legal document analysis inc. case law	n=0	n=0	n=2	n=0	n=6
• Existing Literature	n=0	n=0	n=1	n=0	n=3
• Interviews and focus groups.	n=1	n=0	n=0	n=0	n=1
• Surveys	n=0	n=0	n=0	n=0	n=1
Suggestions & Recommendations: Mitigating legal limitations	n=0	n=0	n=2	n=0	n=4