Policing faces

Routledge
Taylor & Francis Group

Information & Communications Technology Law

ISSN: (Print) (Online) Journal homepage: https://www.tandfonline.com/loi/cict20

Policing faces: the present and future of intelligent facial surveillance

Lachlan Urquhart & Diana Miranda

To cite this article: Lachlan Urquhart & Diana Miranda (2021): Policing faces: the present and future of intelligent facial surveillance, Information & Communications Technology Law, DOI: 10.1080/13600834.2021.1994220

To link to this article: https://doi.org/10.1080/13600834.2021.1994220

Published online: 28 Oct 2021.

INFORMATION & COMMUNICATIONS TECHNOLOGY LAW
https://doi.org/10.1080/13600834.2021.1994220

Routledge
Taylor & Francis Group

Policing faces: the present and future of intelligent facial surveillance

Lachlan Urquhart[a,b] and Diana Miranda[c]

[a]School of Law, University of Edinburgh, Edinburgh, UK; [b]Horizon Digital Economy Research Institute, School of Computer Science, University of Nottingham, Nottingham, UK; [c]Faculty of Social Sciences, University of Stirling, Stirling, UK

ABSTRACT

In this paper, we discuss the present and future uses of intelligent facial surveillance (IFS) in law enforcement. We present an empirical and legally focused case study of live automated facial recognition technologies (LFR) in British policing. In Part I, we analyse insights from 26 frontline police officers exploring their concerns and current scepticism about LFR. We analyse recent UK case law on LFR use by police which raises concerns around human rights, data protection and anti-discrimination laws. In Part II, we consider frontline officers' optimism around future uses of LFR and explore emerging forms of IFS, namely emotional AI (EAI) technologies. A key novelty of the paper is our analysis on how the proposed EU AI Regulation (AIR) will shape future uses of IFS in policing. AIR makes LFR a prohibited form of AI and EAI use by law enforcement will be regulated as high-risk AI that has to comply with new rules and design requirements. Part III presents a series of 10 practical lessons, drawn from our reflections on the legal and empirical perspectives. These aim to inform any future law enforcement use of IFS in the UK and beyond.

KEYWORDS

Facial recognition; Emotional AI; policing; surveillance; law

Introduction

Overview. In this paper, we bring together a novel analysis unpacking both legal and sociological dimensions of future uses of *intelligent facial surveillance* (IFS) by law enforcement. The paper provides a case study of live automated facial recognition (LFR) use by police in public spaces in the UK. In Part I, we present insights from 26 frontline officers on LFR, exploring their concerns and scepticism about the role of this technology. In particular, we consider themes of *ineffectiveness, inaccuracy, distrust, usefulness and intrusiveness*. We then discuss the current law and policy landscape around LFR, particularly the discussing *legal challenges* and *concerns* raised in the UK Bridges cases. These focused on South Wales Police trials of LFR and raised concerns *around human rights, data protection and anti-discrimination law compliance*. In Part II, we advance the discussion to consider future uses of IFS by examining police officer *optimism* around LFR when integrated

CONTACT Lachlan Urquhart lachlan.urquhart@ed.ac.uk

with other technological systems. We discuss the potential integration of LFR with other policing technologies such as body-worn cameras, and the potential for incorporation of face-based EAI capabilities, i.e. systems which seek to read facial expressions, not to identify individuals, but instead to understand their underlying emotive state and intent. This raises legal questions that we explore through the new EU Proposed AI Regulation (AIR), as the world's first comprehensive AI regulatory framework seeking to make AI more trustworthy.[1] We assess the implications of the proposal making LFR a prohibited form of AI in the EU and explore how EAI use by law enforcement will be regulated as a high risk AI system (HRAIS), introducing new rules and design requirements for different stakeholders across the supply chain from providers to users. Part III draws together our consideration of legal issues and empirical insights from operational police officers. We consider the practical issues of deploying LFR and EAI in policing, and develop 10 lessons from current uses and highlight issues that need attention for legally informed IFS in future policing practice.

Background. For centuries faces have been used by law enforcement not just to *identify* but to attempt to *read* states of mind and infer suspicious behaviour.[2] LFR aims to detect and map facial features from audio-visual footage. This is done in order to produce a template that is compared with police curated watchlists to *identify* individuals. Despite the recent attention facial recognition has faced in the press, policymaking and in scholarship, this is a longstanding area of technology development.[3] For example, Japanese IT firm NEC has been developing facial recognition technologies since the Osaka World's Fair in 1970.[4] However, with advances in machine learning and computer vision techniques, visual surveillance mechanisms are being coupled with biometric systems in order to *automate suspicion* and augment human policing capabilities.[5] Legal and surveillance scholars have been raising concerns about the implementation of facial recognition, namely the implications for public space interactions and categorisation of suspicion.[6]

[1]Even if the UK is no longer a member state, this regulation remains relevant because the EU envision it being a gold standard around the world for regulation of AI and thus it will set standards (in the same way the GDPR has). More directly, it remains relevant to the UK because the scope of the law applies to organisations providing services to EU organisations and seeking access to the EU marketplace (see Art 2).

[2]Simon Cole, *Suspect Identities: A History of Fingerprinting and Criminal Identification* (Harvard University Press, 2001); Simone Brown, *Dark Matters: On the Surveillance of Blackness* (Duke University Press, 2015). Diana Miranda, 'Identifying Suspicious Bodies? Historically Tracing the Trajectory of Criminal Identification Technologies in Portugal' (2020) 18(1) Surveillance & Society 30–47.

[3]Guardian News and BBC Portals on Facial Recognition <https://www.theguardian.com/technology/facial-recognition> and <https://www.bbc.co.uk/news/topics/c12jd8v541gt/facial-recognition> all URLs last accessed 16 July 2021.

[4]Kelly Gates, *Our Biometric Future – Facial Recognition Technology and the Culture of Surveillance* (New York University Press, 2011).

[5]Peter Fussey, Bethan Davies, Martin Innes, 'Assisted' Facial Recognition and the Reinvention of Suspicion and Discretion in Digital Policing' (2021) 61(2) The British Journal of Criminology 325–44 <https://doi.org/10.1093/bjc/azaa068>; Diana Miranda, 'Body Worn Cameras on the Move: Exploring the Contextual, Technical and Ethical Challenges in Policing Practice' (2021) Policing and Society <https://doi.org/10.1080/10439463.2021.1879074>.

[6]Gates (n 5); Mitchell Gray, 'Urban Surveillance and Panopticism: Will We Recognize the Facial Recognition Society?' (2003) 1(3) Surveillance & Society 314–30; Lucas Introna and David Wood, 'Picturing Algorithmic Surveillance: The Politics of Facial Recognition Systems' (2004) 2(2/3) Surveillance & Society 177–98; Kyriakos Kotsoglou and Marion Oswald, 'The Long Arm of the Algorithm? Automated Facial Recognition as Evidence and Trigger for Police Intervention' (2020) 2 Forensic Science International: Synergy 86–89; David Lyon, *Surveillance Society: Monitoring Everyday Life* (Open University Press, 2001); Clive Norris, 'From Personal to Digital: CCTV, the Panopticon, and the Technological Mediation of Suspicion and Social Control' in David Lyon (ed), *Surveillance as Social Sorting – Privacy, Risk and Digital Discrimination* (Routledge, 2003); Gavin Smith, 'The Politics of Algorithmic Governance in the Black Box City' (2020) Big Data & Society 1–9; Rebecca Venema, 'How to Govern Visibility?: Legitimizations and Contestations of Visual Data Practices after the 2017 G20 Summit in Hamburg' (2020) 18(4) Surveillance & Society 522–39; Joe Purshouse and Liz Campbell,

In particular, by perpetuating forms of profiling and reinforcing categories of suspicion, groups that are already disproportionally subject to more control are significantly targeted by these systems.[7] Concurrently, concerns around police use of facial recognition also relate to (un)reliability, (in)effectiveness and (in)accuracy when identifying faces in the crowd.[8] Such concerns led to a ban on the use of LFR in several cities in the US (San Francisco, Oakland, etc.), alongside companies calling for bans on police use of these systems, including Google, Amazon, Microsoft, and IBM.[9] More recently, in the wake of the proposed AIR, the European Data Protection Supervisor, European Data Protection Board and European Parliament have all called for stricter regulation of LFR and Emotional AI technologies in public spaces, particularly for law enforcement.[10] Interestingly, the EDPS/EDPB Opinion raises concerns beyond just faces, but to a wider reading of biometrics in public too, indicating future concerns of how AI systems are used to read bodily features more broadly including 'gait, fingerprints, DNA, voice, keystrokes and other biometric or behavioural signals'.[11] In the UK context, British police forces, such as South Wales Police (SWP) and the Metropolitan Police Service (MPS) have been early adopters. MPS has been trialling LFR in events and crowded public spaces in London since 2016 and SWP has been using LFR in trials since 2017 and 2018 in high streets and at concert arenas. We fully discuss how NEC's NeoFaceWatch system was deployed by SWP in Part 1.2.

Whilst there is extensive discussion of LFR in this paper, it is only one example of what we term *intelligent facial surveillance* (IFS). We use the concept of IFS in this paper to begin moving beyond current debates solely focused on LFR, and we believe there is value in the notion of IFS to provide long term reflections and to adopt a wider framing of AI-enabled surveillance targeting the face in law enforcement. We anticipate future forms of IFS beyond public space CCTV such as drones, body-worn cameras (BWCs), dashboard cams or smart home cameras (e.g. Ring partnering with the police

'Privacy, Crime Control and Police Use of Automated Facial Recognition Technology' (2019) 3 Criminal Law Review 188–204.

[7]Lucas Introna and Helen Nissenbaum, *Facial Recognition Technology: A Survey of Policy and Implementation Issues* (Lancaster University Working Paper, 2010); Clare Garvie, Alvaro Bedoya and Jonathan Frankle, *The Perpetual Line-up: Unregulated Police Face Recognition in America* (Georgetown Law, Center on Privacy & Technology, 2016); Damien Williams, 'Fitting the Description: Historical and Sociotechnical Elements of Facial Recognition and Anti-Black Surveillance' (2020) 7(1) Journal of Responsible Innovation 74–83.

[8]Gates (n 5); Information Commissioner Office, *ICO Investigation into How the Police Use Facial Recognition Technology in Public Places*. Hereinafter 'ICO 2019a' <https://ico.org.uk/media/about-the-ico/documents/2616185/live-frt-law-enforcement-report-20191031.pdf>; Information Commissioner Office, *Live Facial Recognition Technology – Police Forces Need to Slow Down and Justify its Use*. hereinafter 'ICO, 2019b' <https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/10/live-facial-recognition-technology-police-forces-need-to-slow-down-and-justify-its-use/>; Introna and Nissenbaum (n 8); Surveillance Camera Commissioner, *Surveillance Camera Commissioner Annual Report 2017/2018*. (SCC, 2018) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/772440/CCS207_CCS1218140748-001_SCC_AR_2017-18_Web_Accessible.pdf>. Surveillance Camera Commissioner, *Facing the Camera*. (SCC, 2020) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/940386/6.7024_SCC_Facial_recognition_report_v3_WEB.pdf>.

[9]Antoaneta Roussi, 'Resisting the Rise of Facial Recognition' (2020) 587 Nature 350–53.

[10]European Parliament, *Motion for a European Parliament Resolution on Artificial Intelligence in Criminal Law and its Use by the Police and Judicial Authorities in Criminal Matters* (European Parliament, 2021). <https://www.europarl.europa.eu/doceo/document/A-9-2021-0232_EN.html>.

[11]European Data Protection Board and European Data Protection Supervisor, *EDPB-EDPS Joint Opinion 5/2021 on the Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act)* (EDPS-EDPB, 2021) <https://edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-52021-proposal_en>.

in the US and UK).[12] We argue IFS can also incorporate non-identifying applications focused on intentionality and state of mind, specifically *emotional AI*.[13] Emotion sensing has been used in advertising and commercial contexts to date,[14] but is also emerging in law enforcement through the iBorder Ctrl[15] and VibroImage.[16] Aligning LFR and EAI with smart city initiatives can lead to troubling applications in law enforcement, e.g. Uyghurs being targeted by these systems in police stations in Xinjiang, China.[17] Avoiding this kind of future in the UK is a key motivation of this paper, and the current focus on identification based harms around LFR means there is a risk these types of systems go unaddressed.[18] We now turn to our officer perspectives on current uses of IFS through their insights on LFR.

Part I – present uses of intelligent facial surveillance

1.1. Frontline policing perspectives

We will now discuss the perceptions of British frontline police officers on the use of LFR. In total 26 semi-structured interviews were conducted with police officers from two British Police forces in different geographic locations (South and North of the UK).[19] Due to confidentiality reasons we cannot name these forces directly, however, they were selected because they were in the process of implementing a range of new visual surveillance technologies. We sought to understand the attitudes and perceptions of frontline officers around current and future uses of LFR in particular. The police officers were selected to ensure a diversity of ranks, age, genders, patrol location areas (both urban and rural) and years of experience. All the participants were informed about the aims of the project, consented freely to being involved and were briefed on the aims of the study and they could withdraw at any time.[20] These interviews, conducted between 2018 and 2019, lasted 45 minutes on average within police stations or headquarters, were audio recorded and transcribed verbatim, without recording participants' names. The names presented below are pseudonyms. The data was analysed and coded following a thematic

[12]Met Police, *Amazon Ring Internet-connected Camera-enabled Doorbells: Freedom of Information Request* (Met, 2020) <https://www.met.police.uk/foi-ai/metropolitan-police/disclosure-2020/january/amazon-ring-internet-connected-camera-enabled-doorbells/>.

[13]Andrew McStay and Lachlan Urquhart, '"This Time with Feeling?" Assessing EU Data Governance Implications of Out of Home Appraisal Based Emotional AI' (2019) 24(1) First Monday <https://doi.org/10.5210/fm.v24i10.9457>.

[14]Andrew McStay, *Emotional AI* (Sage, 2018); Luke Stark and Jesse Huey, 'The Ethics of Emotion in AI Systems' (2021) FAccT '21: Proceedings of the 2021 ACM Conference on Fairness, Accountability, and Transparency 782–93.

[15]Javier Sánchez-Monedero & Lina Dencik, 'The Politics of Deceptive Borders: 'Biomarkers of Deceit' and the Case of iBorderCtrl' (2020) Information, Communication & Society <https://doi.org/10.1080/1369118X.2020.1792530>.

[16]James Wright, 'Suspect AI: Vibraimage, Emotion Recognition Technology and Algorithmic Opacity' Science, Technology and Society (2021) <https://doi.org/10.1177/09717218211003411>.

[17]Jane Wakefield, 'AI emotion-detection software tested on Uyghurs' (2020) BBC News <https://www.bbc.co.uk/news/technology-57101248>.

[18]Despite this, we have had recent calls from EU bodies to ban emotion sensing under the AI Act. See European Data Protection Supervisor and European Data Protection Board, *Joint Opinion 05/2021 on the Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act)* (EDPS/EDPB, 2021) <https://edpb.europa.eu/news/news/2021/edpb-edps-call-ban-use-ai-automated-recognition-human-features-publicly-accessible_en>.

[19]Diana Miranda, *Evidence to Justice Sub Committee on Policing: Facial Recognition: How Policing in Scotland Makes Use of this Technology* (Scottish Parliament, 2020) <https://archive2021.parliament.scot/S5_JusticeSubCommitteeOnPolicing/Inquiries/JS519FR25_Dr_Miranda.pdf>.

[20]This study was approved by Keele University Board of Ethics.

approach utilising principles of analytic induction, i.e. using rounds of analysis to systematically refine the thematic codes.

When discussing scenarios of LFR use our participants' position was mainly one of scepticism and disbelief in the technology. This is illustrated by Police Constable (PC) Amy (2 years of service), who felt even if it would be useful for police forces to incorporate FR capabilities in visual surveillance systems, such use was not perceived as realistic *at present*:

> I don't know how useful or how much we would use something like that. Obviously, there are times where we get, say, CCTV footage of somebody who's committed a theft, and if people can't identify that person … Obviously, it would probably come in handy in cases like that, and you could get a higher detecting rate, **but I can't see that happening any time soon**. **Maybe that's me being sort of sceptical**.

In order to explore some of the concerns and elements of uncertainty raised by police officers, we observed the following themes: ineffectiveness, inaccuracy, distrust (1.1.1), usefulness (1.1.2) and intrusiveness (1.1.3).

1.1.1. Ineffectiveness, inaccuracy and distrust

Despite the different applications of LFR, such technology is often portrayed by police forces as an important tool in the fight against crime and as a valuable and neutral tool to aid policing.[21] This was particularly evident in the study developed by Fussey, Davies and Innes[22] during the MPS trials in London, where 'despite awareness of potential technological limitations', the levels of trust and belief in LFR as infallible and accurate were high.[23] In their words, 'throughout the MPS trials, a commonly articulated and prevailing view was one of faith in LFR systems to enhance policing, but the challenge being in proving its worth *externally*'.[24] Our frontline officers are part of this external audience and our data shows they remain unconvinced about LFR.

Our participants questioned the portrayal of objectivity and neutrality often associated with LFR. They also raised concerns in relation to the accuracy and effectiveness of LFR. Similarly to scholars[25] and policymakers,[26] our participants remained sceptical of its current uses and, in particular, showed disbelief and distrust in LFR technical capabilities. Portraying it as ineffective, Sgt (Sergeant) Lawrence (12 years of service) argued:

> facial recognition is **pretty terrible** from what I've seen of it. I've seen it work a couple of times and it's come out with all sorts of **random decisions** and … so I don't think facial recognition technology is where it needs to be at the moment.

PC John (9 years of service) also discussed the current quality of footage and how more technological improvement is needed for cameras to operate effectively: 'In terms of facial recognition, I'd imagine there might need to be some improvement in relation to the quality of footage. (…) they're probably going to struggle to get decent facial recognition.'

[21]Met Police, *Live Facial Recognition Resource Page* (Met, 2021) <https://www.met.police.uk/advice/advice-and-information/facial-recognition/live-facial-recognition/>.
[22]Fussey, Davies and Innes (n 8) 14.
[23]ibid.
[24]ibid.
[25]Introna and Nissenbaum (n 10).
[26]ICO (n 11); Surveillance Camera Commissioner (n 11).

This theme is also discussed by Fussey, Davies and Innes[27] in relation to the quality of input data impacting the system's effectiveness. The custody images often used by the system differed significantly in standard and resolution, having an impact on LFR performance. In their words: 'Because they were "naturalistic" with people, sometimes smiling or squinting or tilting their heads at an angle, this affected the shape of their faces and, therefore, the algorithm's ability to analyse them effectively.'[28]

Nonetheless, the scepticism of our participants, as members of 'an external audience', was not only associated with direct experiences but also with fictional representations of technology use. When reflecting about the process of searching for faces in a database, PC Larry mentioned: 'I honestly don't know if the technology is like they make you believe in a Hollywood film where they can go through this massive database and go, oh, that's so-and-so, he's a terrorist, because we've got his footage.' This position of scepticism was also linked to the lack of trust on a process of decision-making that involves both human and non-human actors. Our participants were hesitant to show trust in a technology that is automated and dictated by non-human actors such as computers (contrary to other elements of biometric identification). According to Sgt Patricia (14 years of service):

> I don't know how much I'd trust that, because … Well, the only two things we go off now are DNA and fingerprinting, and both of those things are individual to the person. I don't know how much I would trust technology if facial recognition … Because you're relying on a computer, aren't you … ?.

1.1.2. Usefulness

The use of such technologies not only is deemed ineffective but also too expensive at a time of budget constraints. Our participants acknowledged there is a need to keep up with technological development; however, such investment comes at a high price. As mentioned by PC Kevin (12 years of service), based in a firearms unit:

> I think if you were to have an open chequebook, the possibilities for technology and policing, you'd be like Robocop, you would have so much ability to do things. But it's just that cost, and sometimes you look at it and you roll your eyes.

In particular, our participants highlighted the significant financial costs associated with the potential implementation of LFR systems. As stated by Sgt Felicity (18 years of service) when questioned in relation to the use of this technology: 'it sounds expensive, so that is a no'. This was also illustrated by Fussey, Davies and Innes[29] in their study with both MPS and SWP, as the lack of human resources had impacts on the use of LFR. For instance, despite the alert of possible matches to different units, the teams were not available to react to these matches. Indeed, 'constraints imposed by the available human resources to service the 'demand' created by the LFR system moderates simplistic claims that such technologies can address austerity restrictions by replacing policing functions'.[30]

[27]Fussey, Davies and Innes (n 8).
[28]ibid 12.
[29]ibid.
[30]ibid 16.

Overall, from the perspective of our participants, the possibility of incorporating FR capabilities in visual surveillance systems did not seem plausible, at least currently. As stated by PC Ross:

> Possibly a very long way in the future because it's going to be public service in the public sector, it's not going to be well funded, and I don't think we're going to see that for a very long time. (…) I don't know enough about facial recognition software until it's very common, it would be nice to see it, but it will come with its own issues …

Our participants also acknowledged the availability of other technologies that are already used for identification purposes, in particular mobile fingerprint devices. Such technological devices already serve the purpose of recognising and identifying an individual. In the words of Kevin 'we always had fingerprint pads. If you said you're John Smith and you go, right, okay, scan your finger there, right, it's saying you're not John Smith, you're Dave Smith, John's brother, or whatever'. The same is reiterated by PC Andrew (5 years of service) and PC John (9 years of service), respectively:

> I'm sure you could talk to somebody who would tell you the facial recognition would be brilliant, but if we've any concerns about a person's identity, we just run their fingerprints, you get it that way as well. (Andrew)

> The same thing, we've got the **fingerprint scanner** that can probably do the same job before you've got facial recognition. You've got to look at your fingerprints first. (John)

The sceptical views of our participants also highlighted different operational and contextual challenges faced with the use of technologies. Some police officers claimed LFR would not be the most relevant tool in the context in which they operate. In the words of PC Daniel, LFR 'is only used in the most elite of elite', namely in megacities like London. When discussing this with PC Andrew, he also argued that the investment in such technology would not be particularly useful in the metropolitan area he works (a city with a population of approximately 200,000 inhabitants). Considering the size of this area and the type of criminal activity they often face, this participant stated they tend to know the members of the public they often interact with, reducing the value and relevance of technologies such as LFR:

> I don't know how useful it would be in [given city] in relation to, you know … even though it's a city, it's probably a big town, you know, you will know the majority of the bad men and women that you deal with, it's the same offenders kind of again, so I don't think you would need facial recognition. When you're talking about the Metropolitan Police, they're going to be dealing with terrorist incidents, you know, organised criminal gangs. Well, don't get me wrong, we have that up here, but they're probably on a lesser scale, so I think that they could probably use their money elsewhere more effectively.

The same concern applies to rural settings and the debatable usefulness and relevance of LFR in areas where people normally know each other. Even if initially PC Matthew revealed optimism with the potential use of FR (in particular when considering large events), since he is based in a rural setting, he did not perceive the use of this technology as relevant in such context due to their interactions with the public occurring at 'a smaller scale'. In his words:

> obviously I think in terms of use maybe it wouldn't have quite as big an impact being kind of a rural setting because the people you encounter tend to be on a smaller scale, one on one maybe as opposed to large situations where people's images are being recorded.

Lastly, even if LFR could be considered and applied in such settings, the participants raised some practical concerns in relation to the quality of the internet connection they have available. As mentioned by Sgt Nelson:

> with our radios we struggle [with reception] in certain parts, especially if you go more rural (…) So, if we're having a live feed of a camera, that backs up somewhere else, then I would suggest that you would struggle with the connection sometimes.

However, even in urban areas, there are often still technical difficulties limiting the use of AFR. As portrayed by Fussey, Davies and Innes (2021), even in central London radios would often fail inside the AFR-equipped vans, limiting the operators' capacity to react and communicate with the street-based intervention team.

1.1.3. Intrusiveness

The results of a national survey published by the Ada Lovelace Institute[31] revealed that the British public is mainly concerned with privacy infringements, surveillance, consent and unethical use of FR by the police. Intriguingly, such concerns were shared by the police officers interviewed. The need for safeguards prior to LFR implementation was raised as crucial, as it was considered by our participants that there are significant potential impacts on the legal and human rights of citizens.

PC Matthew was particularly concerned with the legal challenges and privacy implications of using LFR: 'obviously from the public's point of view I'm sure there'd be a concern about invasion of privacy and everything else'. Sgt Simon (12 years of service) also raised some concerns in relation to data collection and the need to follow due process and clearly explain the purposes of LFR, so it is not deemed invasive by members of the public:

> There're processes in place, and those processes are there for good reason because if you could just dip in and out all of that, you could … Yes, it's quite scary I think (…) keeping up with what's relevant, but it's got to be relevant and useable and useful to us, and **not being invasive**. Everything's got to be done for a reason. We got to **be able to justify** what we've done, I think.

In particular, our participants voiced concerns on how LFR might be deployed and the need to clarify the purpose of using this technology. If used for recognition and identification purposes, the police officers argued that is not needed when dealing with law-abiding citizens. This is particularly relevant if we consider a scenario of body-worn cameras with LFR capabilities[32] as a future IFS system. Still in the words of Sgt Simon*:*

> We don't need to know the identity of everybody because most of the people we deal with are law abiding. If you're walking down the street, **I don't need to know who everybody is**. It might be beneficial because you might find Joe Bloggs who's wanted (…) but actually is that right, … because that's what you do, **you are surveilling everybody**, and that's not the spirit of the camera.

[31]Ada Lovelace Institute, *Beyond Face Value: Public Attitudes to Facial Recognition Technology* (Ada Lovelace, 2019) <https://www.adalovelaceinstitute.org/report/beyond-face-value-public-attitudes-to-facial-recognition-technology/>.
[32]Miranda, (n 8).

PC Ian also reiterated this by highlighting that there is no need to record every interaction with members of the public, by comparing their professional practice with the process of gathering research data:

> I think that [LFR] would be better not necessarily on the officer's personal body-worn camera because you're not going to walk about with it on 24 hours a day. (…) You don't have to record every interaction. How many conversations we have today? There's many but you won't record them all. Would you walk about as a researcher and do what you do, recording everybody's behaviour and everybody's … ? You know what I mean? It's an interest you have but is it valuable or no? Or is it just certain times you want to do it, like now? **The camera's the same.**

This analogy is interesting, where in performing empirical research and data collection, researchers need to abide by ethical approval procedures, safeguards around data collection and storage, protecting participants with consent and transparency of behaviour. There are also particular concerns related to data management and how footage is collected and stored in a scenario of constant collection. According to our participants, footage would need to be collected continuously to enable LFR and concerns were raised in relation to its security and storage. According to Sgt Nelson (13 years of service):

> I guess that would have to be done then live, so if we're going to have facial recognition technology, you'd have to be **recording the whole time** to enable that. (…) We'd have to have a system then where we're recording live, picked up the whole time, otherwise the person we want, that it recognises, will be gone by the time we've even registered it. (…) That brings in the problems about us having to record the whole time (…) And **that presents a whole new problem**, doesn't it, **of security**.

This was deemed to be particularly problematic if body-worn cameras were to incorporate LFR, as police officers agreed they should only record specific interactions with these devices. However, participants believe LFR will become common practice in the future and that specific guidance is needed on how to manage the data effectively. For instance, Insp Oliver was convinced that LFR will eventually be implemented and highlighted the need of proportionate use:

> I would bet my pension on it [LFR]. (…) I would like to think, anyway, that it would be used **proportionately**. I mean it would be used to investigate more major crime. (…) Once again, it will be all about managing the data and how that's looked after. And whether it's dealt with proportionately at the time.

These themes of proportionality and scale of crimes where LFR should be used for are unpacked in the legal sections below. Overall, when considering the implications of using LFR, our participants questioned how human rights might be compromised and, in particular, if the use of this technology for law enforcement purposes is in the public interest. Our participants questioned if the use of such tools would be proportionate, in particular, if the purpose of use is not clear. As illustrated by PC Daniel (5 years of service):

> It would be well in the future [the implementation of LFR]. I think it would be extremely useful. But for us, in an ideal world imagine your camera could recognise that person without you even going up and asking for their details and that person's wanted? Yes, that would be very handy. But I imagine there'd be **a lot of questions from the public**

> because it would be **scanning all the time**. (…) It would definitely be **invasive** because if members of the public knew that this was scanning your face and stuff like that I would be – even though I've done nothing wrong – you'll probably be, your reaction is, oh the police are coming. I'll just walk away because I don't want to be scanned. Like, it's almost like a futuristic movie that you're watching where these robots can down scan people, you know what I mean? (…) **It would be great to scan everyone but morally I don't think that's right at all.**

Building on the issues previously explored, our participants were also concerned with how this technology might impact public confidence (or lack of) in police work. If LFR is perceived negatively by the public, there is the need to clearly justify its purposes and uses to avoid damaging public's perception of the police. In the words of Sgt Simon:

> I think that's quite a big step because then if you're going down that route [LFR], you're looking at having this on all the time almost. Not that has to be on, but it's always there in the background (…) I think that would perhaps damage the perception of the police with the public because it's less difficult … If it's always recording and they know it's always evidence gathering, it just looks like we're sleeping. I think if it happens it's going to be a long way off, and I think it would need to be really justified as to why. Really justified. I don't think I'd be keen on that.

As we see below in Parts II and III, changes prompted by the Bridges cases have led to initiatives from the College of Policing to create a framework for LFR use that addresses public concerns in the future. But this sits in contrast to shifts in the EU AIR, which seeks to prohibit LFR by default, and only use in specific circumstances (detailed in Part II).

1.2. Legal perspectives

In this section, we contextualise the emerging legal framework around police use of facial surveillance in the UK by the police. Legal analysis involved examining primary sources in a doctrinal manner, namely legislation and case law pertaining to LFR. Thus, the Bridges cases, proposed EU AIR and commentary around these were considered. Our participants often point towards the lack of legal certainty surrounding the use of LFR, including around invasiveness. This section explores the Bridges High Court and Appeal Court test cases and unpacks how they will direct future police use of LFR.

Bridges v South Wales Police: High Court (HC)

One of the key resources in discussing legality of the use of LFR is the original High Court[33] and the Court of Appeal[34] *Bridges v South Wales Police* cases. We briefly consider the former before turning to the latter.

The original case was decided on 4 September 2019, brought by civil liberties campaigner Edward Bridges. He filed the claim on the basis of two occasions where he was recorded by Automated Facial Recognition (AFR) Locate in Cardiff,[35] an example of LFR systems. There were 50 trials run using the *AFR Locate* system by South Wales Police

[33] *Bridges, R (On Application of) v The Chief Constable of South Wales Police [2019] EWHC 2341 (Admin)* (04 September 2019) (hereinafter 'HC').

[34] *R (on the application of Edward Bridges) v The Chief Constable of South Wales Police v The Secretary of State for the Home Department, The Information Commissioner, The Surveillance Camera Commissioner, The Police and Crime Commissioner for South Wales [2020] EWCA Civ 1058*, 2020 WL 04586697 hereinafer ('CoA').

[35] Para 34 CoA – they assume/accept he was, due to data retention etc, this cannot be proven.

(SWP), itself based on the NEC/North Gate Public Services NeoFaceWatch system.[36] It is estimated it had scanned over 500,000 faces during these trials between 2017 and 2018, scanning up to 50 faces per second.[37] They were overtly photographing members of the public in real time via CCTV (static or mobile on vans). They then analysed the images to detect faces and then extract facial features to create a biometric template consisting of numerical measurements. These were then checked against a watchlist database of between 400 and 800 faces.[38] Primarily based on a custody photograph database, this includes a variety of individuals, including those with warrants, escaped prisoners, suspects, vulnerable people and those needing protection like missing persons in addition to those of interest for intelligence or who prompt concern by being at an event.[39]

To briefly consider how this system works, it looks for a match and presents a similarity score with a % of the likelihood of this being the individual in question. The threshold % value is set by the user (to manage false positives and negatives),[40] and if there was no match, the facial image and biometric template are deleted immediately and automatically[41] (although CCTV footage is retained for 31 days and then automatically deleted).[42] Once a match is identified, a police officer reviews this and decides on further action, e.g. intervention.[43] During trials the police would notify the public of the use of *AFR Locate* via social media channels, large posters in a 100 m radius of the cameras, on the SWP website and on postcard-sized notices given to the public.[44] The facts of the original Bridges case have been discussed fully by numerous commentators.[45] For our purposes, we focus briefly on the human rights requirements, as they help to explain the balancing exercise necessary in Art 8(1) and (2) of the ECHR.

European Court of Human Rights jurisprudence is relevant in this case as UK courts have to consider it under sections 2 and 6 of the UK Human Rights Act. Art 8(1) of the ECHR states 'everyone has a right to respect for their private and family life' but this is a qualified right under Art 8 (2). It then states that public authorities should not interfere with the right *except* if it is in *accordance with the law*[46] and *necessary in a democratic society* (e.g. for one of legitimate goals of national security, prevention of disorder and crime or public safety). Case law has established that *necessity* also includes an assessment of *proportionality* of the action to the legitimate aims being pursued.[47] If the Art 8(2) safeguards cannot be satisfied, then there will be a violation of Art 8(1) and a breach of the Convention right.

In this case, the activities of SWP triggered Art 8(1) and infringed it for a number of reasons.

[36]Para 10 CoA.
[37]Para 16 CoA.
[38]Para 13 CoA.
[39]Para 13 CoA.
[40]Para 7–10 CoA.
[41]Para 93 CoA (something that can help with adequacy under the law).
[42]Para 17–18 CoA.
[43]Para 15 CoA.
[44]Para 19 CoA.
[45]Kotsoglou and Oswald (n 9).
[46]*Malone v UK* 1984 7 EHRR 14.
[47]*Dudgeon v UK* 1981 7525/76 s51–53; *Z v Finland* 1997 22009/93 s94.

- The police use of AFR Locate was not 'expected and unsurprising', unlike with the mere taking of photos in public.[48]
- The storage of data[49] by police was an interference, especially because it involved intrinsically private data like biometrics.
- The fact data was collected in public or only used for a short period of time did not legitimise the AFR Locate system either (i.e. Art 8 is not only relevant when data is retained for a long time).

The case focused on whether this infringement of Art 8(1) could be justified under Art 8(2). The requirement of Art 8(2) for any infringement to be 'in accordance with the law' is important as the law should be *accessible and foreseeable* in order to guard against arbitrariness and too much discretion by the state.[50]

On those points, in the original case, it was deemed in *accordance with the law* because of common law powers police had around prevention and detection of crime. AFR Locate is subject to the Data Protection Act 2018 and UK Protection of Freedoms Act 2012 alongside also the statutory code of practice: the Surveillance Camera Code.[51] The cameras were not deemed physically intrusive methods of obtaining data (unlike seizures from homes) and watch lists were deemed legal under the UK Police and Criminal Evidence Act 1984.[52] It was deemed *necessary* and *proportionate* in part because it was not permanent and focused on a specific geographic area. Also, the public were informed it was operating and it had specific targets it sought to identify. As we will now see, some of these points were contested in the Court of Appeal case, and we reflect on concerns around anti-discrimination and data protection laws below, as the CoA case has had less academic analysis thus far.

Bridges v South Wales Police: Court of Appeal (COA)

Following an appeal supported by Liberty, in Aug 2020 a judgment was handed down by the Court of Appeal which deemed the use of AFR Locate unlawful. Whilst the case covered 5 grounds, we focus on grounds 1, 3 and 5 on which the appeal succeeded.[53]

Ground 1 found AFR Locate 'was not in accordance with the law'. Here, the CoA was concerned there was too much discretion for police powers namely around discretion for who is added to *watchlists and locations where* AFR Locate *is deployed*.[54] Thus 'policies do not sufficiently set out the terms on which discretionary powers can be exercised by the police and for that reason do not have the necessary *quality of law*'.[55] The CoA reflects on three areas of law in the UK that could provide 'accordance with the law'. Whilst the

[48] *Wood v Commissioner of Police for the Metropolis* [2009] EWCA Civ 414 – mere taking of a photo in public (by anyone incl. police) did not engage Art 8 unless aggravating/harassing/hounding circumstances for a subject. But in this case, still had to consider full purpose of collection (e.g. if collecting to retain/use) and explain that they will be used in this way.

[49] *S v UK 2009 48 EHRR 50.*

[50] *Re Gallagher [2019] 2 WLR 509* 'it should not 'confer a discretion so broad that its scope is in practice dependent on the will of those who apply it, rather than on the law itself' (para 17); *S v UK* para 95.

[51] Para 80 HC.

[52] *R (Catt) v Association of Chief Police Officers [2015] AC 1065.*

[53] Ground 2 failed as they deemed it to be proportionate see para 134–144, if it had been in accordance with the law; ground 4, the challenge to the lawful basis for processing as required in s35 and quality of documentation required under s42 Data Protection Act 2018 was not considered, as the DPA 2018 was not in force at the time of the trials.

[54] Para 91 CoA.

[55] Para 94 CoA.

DPA 2018 Part 3 is a key area of law around lawful and fair processing and necessity of sensitive processing, they conclude it is not sufficient by itself.[56] Similarly, the Surveillance Camera Code provides scope to deal with aspects of the technology as it applies to LFR (as per s29 of the Protection of Freedoms Act 2012).[57] For example, whilst not currently providing guidance on this, it could be a site for policy on criteria for watchlists and location of deployments,[58] and the Commissioner has already started making inroads into this on the issue of watchlists.[59] Lastly, local police policies were questioned as not having sufficient quality of law too, as they do not provide sufficient guidance of terms for placing individuals on watchlists or locations where AFR Locate was to be deployed.[60] For example, with locations, the police stated AFR Locate would be used at all events including sporting and music but the court was worried that this is not a set of criteria and that it is overly broad.[61] They raised similar concerns with the judgement of why someone is added to a list, particularly for category of 'other persons where intelligence is required' where the court says '*In effect it could cover anyone who is of interest to the police. In our judgement, that leaves too broad a discretion vested in the individual police officer to decide who should go onto the watchlist*.'[62]

Ground 3 found that the data protection impact assessment (DPIA) required under s64 of the UK Data Protection Act 2018 was inadequately done. One issue was the DPIA was written assuming Art 8 was not engaged, when in fact it was, and it was infringed. Secondly, the DPIA did not deal with biometric data of members of the public who were captured by AFR Locate but not present on watchlists. As the court states, the use of AFR Locate was not in 'accordance with the law' because of wide discretion around 'the selection of those on watchlists, especially the "persons where intelligence is required" category, and the locations where AFR Locate may be deployed' thus it breached Art 64 (3)(b) and (c) DPA 2018 as it 'failed properly to assess the risks to the rights and freedoms of data subjects and failed to address the measures envisaged to address the risks arising from the deficiencies we have found'.

Ground 5 found that the use of AFR Locate did not comply with their public sector equality duty (PSED) under s149(1) Equality Act 2010.[63] This is due to the lack of investigation in the equality impact assessment by the police if AFR Locate enabled *indirect* discrimination (they did consider direct).[64] They had not investigated if there were risks from AFR Locate based on race or sex bias, which has impacts on BAME communities in particular.[65] The complaint was based on the lack of fulfilling the duty to investigate

[56]Para 104 CoA.
[57]Para 110 CoA.
[58]Para 118 CoA.
[59]Para 118 CoA and Surveillance Camera Commissioner (2020).
[60]Para 121–129 CoA.
[61]Para 130 CoA.
[62]Para 124 CoA.
[63]The PSED is a response to BAME/police relations after the Stephen Lawrence Inquiry. The fact this was not done properly by the police is even more concerning para 179 CoA.
[64]Para 164 and 167 CoA.
[65]It states:

> A public authority must, in the exercise of its functions, have due regard to the need to – (a) eliminate discrimination, harassment, victimisation and any other conduct that is prohibited by or under this Act; (b) advance equality of opportunity between persons who share a relevant protected characteristic and persons who do not share it; (c) foster good relations between persons who share a relevant protected characteristic and persons who do not share it.

this, as opposed to allegations AFR Locate does perpetuate bias.[66] AFR Locate uses NEC's NeoFaceWatch[67] and testimony from NEC employee witness claims that it is trained with equal numbers of male and female face data and that '*NeoFace Algorithm training data includes a wide spectrum of different ethnicities and has been collected from sources in regions of the world to ensure a comprehensive and representative mix.*'[68] Despite these claims the court was concerned that '*SWP have never sought to satisfy themselves, either directly or by way of independent verification, that the software program in this case does not have an unacceptable bias on grounds of race or sex*.' [69] The presence of human failsafe (i.e. where 2 humans have to consider if they want to respond to a positive match) was not deemed sufficient to discharge their duty.[70] This raises questions about public procurement and need for public sector bodies to scrutinise algos as need to address equality obligations.

Having unpacked the current law and officer perspectives through our examples, we now turn our attention to future optimism from officers around LFR but situate this within the emerging legal landscape. This highlights how face-based surveillance will be subject to growing policy measures that, depending on jurisdiction, either seeks to ban further use (as we see at the EU level with the AI Act), or to mitigate risks and legitimise roll out through policy (at UK Level with College of Policing guidance).

Part II – future uses of intelligent facial surveillance

2.1. Frontline officer perspectives

In this section, we consider *three areas of future use* discussed by our officers, namely around how LFR can be integrated with other policing technologies; how it can be used to deal with policing large crowds; and their concerns about gradual integration shaping public acceptance.

Our participants' position of optimism and confidence was projected into the future. We observed how they see IFS tools impacting their policing practice. They showed confidence in future uses of LFR when it is linked and integrated with other technologies such as CCTV or BWCs. Considering the importance of IFS in their professional practice, participants expect LFR to play a helpful role in future policing. As stated by both Richard (a frontline response officer with 9 years of service) and PC Katherine (10 years of service), most of their work relies on CCTV footage to recognise and identify suspects during investigations. With the improvement of its technical capabilities, a system capable of pointing them in *a* direction could be extremely relevant in the future[71]:

[66]Para 165 CoA:

> It is important to be clear that it is not alleged that the software used by SWP does have that effect. There is no claim brought on the basis of the negative obligations in the Equality Act, not to discriminate (whether directly or indirectly). Rather the complaint is based on an alleged breach of the positive duty to have due regard to the need to eliminate such discrimination.

[67]para 195 CoA.
[68]para 196 CoA.
[69]para 199 CoA.
[70]para 184–185 CoA.
[71]Miranda (n 5).

> If there was **facial recognition software**, (…) that would be a **huge benefit** to us. If we could run pictures through it and it comes up with **matches**, especially in more major investigations, that would be very beneficial. If you are trawling through hours and hours of CCTV footage **looking for a suspect**, if a computer can scan it in minutes for you, it will save a lot of time and make positive identifications …

> I don't know everybody here (…) Just now we get the CCTV and whatever and people, you put them up in the muster room for people to have a look and see if they can identify them and if you had a **computer system** that **can do that for you**, that would be ideal. It would cut your time in half doing your job if people … I just don't know if the quality is up to that. I don't know. I have no idea but if it was it would be ideal. It would be half the battle for us.

The same applies to the potential integration of LFR in BWC, as this would be particularly useful with the footage collected by mobile cameras that can capture facial features with more quality and definition than CCTV systems. In the words of PC Steph (4 years of service) and PC Carol (2 years of service):

> If that technology got good enough that we could really be relying on it then, yes, absolutely because **BWC** is going to **capture somebody's face** a lot better than any CCTV system could. So, yes, as and when that technology really starts to push forward then, yes, I think they would be good (PC Steph)

> Well, CCTV you can't really get here. With the BWC, you're right up close, getting their faces or directly. Because sometimes, with **CCTV**, it's a **bit distorted**, their faces, you can't see. So, it'd be good. The body worns are an excellent tool for going in and getting the faces because it's so clear. (PC Carol)

Nonetheless, such confident and optimistic positions would always be framed around the premise of a future vision where the technology is working effectively and available to help police forces. PC Oscar (14 years of service) illustrated this future vision by saying:

> If that **helps us to do our job**, then yes, I'm all up for that and I think **that is to come**. I don't think obviously that's something that is readily available to us just yet, and I'm pretty sure that's being looked at and designed and if worked on, evolving through other forces potentially. But if Review came back to us a couple of years down the line and said, look, we've got this package now. We have the software upgrade which will allow you to start doing identification via facial recognition from our database, from the cloud, is that something that interests you? I would say, yes please, (…) If that's my only avenue to identify that suspect, then yes, I'm all up for that. It's just another piece of evolution and development which we will obviously match towards, strive towards.

This is particularly relevant when imagining how they will deal with large events (ie. sporting events) and public order incidents in busier, urban areas. As illustrated by PC Matthew (4 years of service) and PC Ian (16 years of service), respectively:

> The more technology we have to **assist** us in our role the better really. I suppose, yes, on a practical level, certainly with maybe **large public** or situations where they'd be going to like a **football match** or something, there'd be a definite need for that technology. (PC Matthew)

> If you are going to an **event or a large crowd** [unclear] that was for that and you had cameras that had that technology on it, well then yes, I can see it. (…) When a lot of people are funnelling through a small gap like a football turnstile … We've got violent football fans. (…) If you had facial recognition at turnstiles at sporting events like football, then these people can be stopped from coming in. (PC Ian)

The participants discussed how the adoption of an emerging technology such as LFR is subject to a process of either acceptance or resistance from both members of the public and police organisations. Several examples were used to illustrate how technologies were accepted in the past and are now used in a daily basis (such as automatic number plate recognition) and how LFR could be just a 'step further' in order to 'read the picture, the image, of the person' in the future (Larry, 12 years of service). Nonetheless, officers agreed that they will face backlash from the public if LFR is not deemed to work effectively. For instance, PC Mark (27 years of service, firearms unit) believed that:

> We will be using a lot in the **future**. I wouldn't say debug it and get one that works but then it is just one of those things that will be **used to fight crime**. I would imagine lots of people would **moan about it to start with**, but I would imagine once we get a system that works properly **we will end up using it**.

Now we turn to the College of Policing Guidance for UK police forces on LFR future, which shares some of this optimism, but as we state, raise some new concerns.

2.2. College of policing guidance

Recent College of Policing (CoP) documentation from Spring 2021[72] outlines a proposed national approach to LFR for law enforcement in the UK. It is extensive but provides useful guidance which aligns with themes that are discussed in the paper (particularly around watchlists, the public sector equality duty and intrusiveness). We treat each in turn below. Even if these suggestions in the guidance change, it nevertheless indicates the optimism around LFR future use at a policy level in the UK.

A. Watchlists

In attending to concerns around vulnerable individuals appearing on watchlists, the CoP raise disability and age as two key attributes of concern. This is not due to vulnerability *per se*, but instead around concerns of how these attributes impact the accuracy and effectiveness of LFR systems. For example, with disability the issue is if subjects have suffered a facial injury or trauma, undergone facial surgery, have features which cannot be recognised. Similarly, with age, the guidance raises concerns around youth offenders under 18 or 13 because their faces change, impacting the reliability of LFR.[73]

As both Bridges cases highlighted, how images come to be included on watchlists was a concern of the courts. CoP Guidance in Part 2.3 details the types of images that can be added. This is a broad list covering police originated and non-police originated images. The latter is particularly where the force does not have suitable images in house. We provide abridged guidance in the table below.

Police Originated Images	Custody images; Individuals wanted by the courts, Those suspected of committing an offence or with grounds to suspect; Those subject to bail conditions, court order or other restrictions; Missing persons at risk of harm;

[72]College of Policing, *Police Use of Live Facial Recognition* (CoP 2021) <https://www.college.police.uk/article/police-use-live-facial-recognition-technology-have-your-say> hereinafter ('CoP').
[73]CoP Part 2.2.3.

	Those presenting harm to themselves or others; Victim, witness or associates.[74] Other: this depends on an assessment examining purposes underpinning why police hold these images, processing limitations, the importance of inclusion and proportionality of using these.
Non Police Originated Images[75]	Does not stipulate exhaustive sources of data but can include from: • law enforcement partners, • public bodies, • private companies, • individuals Types are the same as those listed above, e.g. those wanted by courts, suspects etc. Criteria for inclusion in the watchlist include: • Only with the approval of the authorising officer • Assessment of purposes underpinning why police hold these images, • processing limitations, • importance of inclusion and • proportionality of using these.

This list is problematic given concerns around the role of social media intelligence (SOCMINT) by police and the legalities of sourcing content for investigations from these channels.[76] It also highlights the risks of involving individuals in lateral surveillance practices, as we saw in police investigations following riots in Manchester and London in 2011 (e.g. 'Catch a Looter').[77] Whilst providing criteria for being put on a watchlist, and thus satisfying concerns of the court around the nature of criteria, they can still be questioned on the merits of their breadth. As we will discuss below, there is a contrast with the EU position in the AIR where it lists tighter applications for LFR use.

B. Public sector equality duty

The proposed guidance also suggests how police can address their PSED[78] and how forces can take steps to ensure the accuracy and performance of deployed LFR. They suggest a holistic approach incorporating assessment of the software, cameras, LFR system and authorising officer procedures too.[79] The CoP suggest steps including:

- Conducting and reviewing their equality impact assessment, or similar process;
- Ensuring they are satisfied reasonable steps have been taken to mitigate bias risks, particularly for protected characteristics, e.g. sex, race, religion, belief;
- Ensuring ongoing review of use, performance and utility of PSED mitigation measures;
- Providing oversight of vendor claims about LFR including testing themselves.[80]

[74]CoP Part 2.3.1.
[75]Images not taken under direction of the police.
[76]Lilian Edwards, and Lachlan Urquhart, 'Privacy in Public Spaces: What Expectations of Privacy Do We Have in Social Media Intelligence?' (2016) 24(3) International Journal of Law and Information Technology 279–310; David Omand, Jamie Bartlett and Carl Miller, 'Introducing Social Media Intelligence' (2012) 27(1) Intelligence and National Security Review; Bert Jaap Koops, Jaap Henk Hoepman and Ronald Leenes, 'Open Source Intelligence and Privacy by Design' (2013) 29 Computer Law and Security Review 676. Daniel Trottier, 'Open Source Intelligence, Social Media and Law Enforcement: Visions, Constraints and Critiques' (2015) 18(4–5) European Journal of Cultural Studies 542.
[77]Elisa Pieri, 'Emergent Policing Practice: Operation Shop a Looter and Urban Space Securitisation in the Aftermath of the Manchester 2011 Riots' (2014) 12 Surveillance and Society 1, 38.
[78]s149 Equality Act 2010.
[79]Part 1.5.5 CoP.
[80]Part 1.5 CoP.

As the Bridges CoA case flagged, the interplay between private vendors and police meant that commercial confidentiality and a lack of willingness of vendors to provide information for testing prevented police discharging their PSED.[81] Thus, the desire for oversight is an important commitment, but in practice, the CoP do not provide steps how to materialise this approach in the UK. As discussed below in s2.2, legal obligations in the AIR are targeting this oversight and seeks to change the interactions between public and private sector in the realm of law enforcement.

C. Procedure and discretion

There is a high level of discretion for each police force, where Chief Officers (CO) can create their own policy around LFR.[82] Nevertheless, the CoP establishe harmonised commitments to guide policy development at a national level, and we select some below as they relate to our data and analysis.[83]

Firstly, forces should only use LFR if *less intrusive methods* wouldn't enable the same objectives. Our participants raised a similar point, arguing fingerprinting pads could help to identify individuals in the street just as effectively. They argue this is a less intrusive method that already exists in policing practice which makes it lower cost and does not require additional training (unlike LFR). Touching on this point, the Bridges CoA case reflected on differences between fingerprinting vs. LFR, where they stated the latter involves procurement without the use of force, cooperation or knowledge of subjects and ability to do so on a mass scale.[84] This suggestion also aligns with the AIR provision which puts the emphasis on police to show that the use of LFR is so important that if it was not used, harms would occur.

Secondly, they raise proactive *engagement* with public and community to foster public trust and confidence as key. This again aligns with our empirical perspectives of officers around fears due to negative public perceptions of LFR. It also raises the issue of the PSED not being conducted properly which was a key issue in the Bridges case. The PSED is an obligation brought about by poor police relations with BAME communities after the Stephen Lawrence Inquiry, making the fact it was not done properly with a technology that could be biased against race even more problematic.[85]

Thirdly, ensuring LFR use is in accordance with the law and used overtly in a 'responsible, transparent, fair and ethical way'. Whilst a laudable aim, the challenges raised in the Bridges cases showed issues of ensuring 'in accordance with law' given the need for *quality of law* that appropriately balances human rights with law enforcement goals. Also, the mention of *overt usage* is important, as covert uses may trigger different investigatory power rules,[86] as the CoP recognise. LFR has scope to become part of directed or

[81]Para 199 CoA.
[82]Part 1.1.5.
[83]See Parts 1.6.1 A) – P) CoP.
[84]CoA para 23:

> Facial biometrics bear some similarity to fingerprints because both can be captured without the need for any form of intimate sampling and both concern a part of the body that is generally visible to the public. A significant difference, however, is that AFR technology enables facial biometrics to be procured without requiring the co-operation or knowledge of the subject or the use of force, and can be obtained on a mass scale.

[85]Ruha Benjamin, *Race After Technology: Abolitionist Tools for the New Jim Code* (Wiley, 2019).
[86]Provisions of Regulation of Investigatory Powers Act 2000 not repealed by the IP Act, particularly Part II.

even intrusive covert surveillance operation, so forces need to continue to make it clear to the public that LFR is being used in an overt way.[87] SWP used a number of mechanisms to do this, but if LFR is used in less transparent ways (e.g. less obvious cameras) then the quality of law, namely RIPA, could come into question too. Given existing concerns around transparency, community relations, and reputation damage with *overt* LFR, the risks from *covert* LFR use seem significant for future deployments.

Fourthly, at a mundane level, CoP also highlight the operational policy documents that need to be drafted for the use of LFR by a police force. These are interesting as they show how high level ethical and legal concerns boil down to a series of documents being drafted to legitimise the use of LFR.[88] This includes:

- A flowchart for decision making on LFR use.
- A standardised operating procedure for LFR including criteria for watch lists and imagery sources, guidance what to do when alerts created, location and camera placement, retention periods, ensuring use is overt '*including considerations of prior notification and signage*'.
- Data protection, equality and community Impact assessments
- Training materials.
- A policy document covering processing of sensitive data.

Operationally, this checklist type approach shows lessons learned from Bridges about areas of concern raised there and procedural steps that need to be taken.

2.3. Future legal perspectives: the emergence of the EU proposed AI regulation

In this penultimate section, we consider the *Proposed EU AI Regulation (AIR)*[89] and how it seeks to shape the future of IFS in Europe. AIR seeks to establish new risk based, tiered rules around the use of AI, to create an ecosystem of trust. It largely splits the rules on if AI is prohibited, high risk or minimal risk. It takes a stance on prohibiting AI for live biometric identification in public spaces by law enforcement (i.e. LFR) and provides guidance on law enforcement use of *emotion identification* (i.e. EAI) as high risk. As mentioned in the introduction, we are interested in the role EAI plays in policing and how it might emerge as a near-future IFS tool. AIR provides a useful roadmap of the priority areas and safeguards needed around integrating AI into policing practice in the future. Whilst it may be non-binding for the UK policing due to Brexit,[90] UK firms (AI providers, users, distributors and others) seeking access to the EU market will need to consider impacts of these rules. Moreover, it will remain useful policy guidance for *best practice* around the use of IFS now and in the future, and in order to gain public trust, the UK may seek to align with strategies documented here.

[87] Indeed section 3.1 documents guidance on what kinds of steps should be taken in relation to date, time, duration and location of live AFR usage including, but not limited to locations such as hospitals, places of worship, polling stations, schools or demonstrations. Signage should also be accessible for children.

[88] Part 1.7. CoP.

[89] European Commission, *Proposal For A Regulation Of The European Parliament And Of The Council Laying Down Harmonised Rules On Artificial Intelligence (Artificial Intelligence Act) And Amending Certain Union Legislative Acts COM/2021/206 Final* (2021) <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52021PC0206&from=EN> hereinafter ('AIR').

[90] Although see Art 2 on scope and impact on third countries seeking access to EU market.

2.3.1. LFR as prohibited AI

Art 5 documents types of AI which are *prohibited* from being placed on the EU market, into service or used and includes 'the use of "real-time" remote biometric identification systems in *publicly accessible spaces* for the purpose of law enforcement'.[91] The law takes this provision seriously, with large fines for breaches of 6% of previous year's annual turnover or up to €30m.

Whilst this initially seems to be a ban on the types of LFR discussed in this paper and used by SWP and the MET, this provision is heavily caveated in the subsequent sections. It discusses elements around the purposes of the system, levels of proportionality, impacts on fundamental rights, if it is urgently needed, if EU member state (MS) domestic law permits it, and it tries to place oversight through authorisation from a judge or authority for usage.[92] To explore this further, in terms of purposes for use, it is prohibited unless strictly necessary for purposes such as targeted searching for victims of crime and missing children[93]; preventing threats to life or physical safety such as terrorist attacks[94] and for finding suspects for serious crimes punishable by at least 3 years custodial sentence and covered by the European Arrest Warrant, e.g. terrorism, trafficking in drugs or human beings, murder.[95] This latter point is interesting insofar as it brings in a severity of crime that goes beyond just deploying LFR at an arena or in a high street in the hope of catching shoplifting or antisocial behaviour suspects from a widely framed watchlist (as was the case in Bridges). This removes 'fishing expedition' type uses and reiterates that this is a tool to be used for serious crimes.

In deciding to use LFR, it is important to consider the circumstances surrounding use, particularly issues of 'seriousness, probability and scale of harm' that could result. Interestingly, it frames these in the negative, i.e. in the absence of the use of the system, what harms would occur? There is also need to consider the fundamental rights and freedoms of *all* subjects implicated by it, i.e. not just suspects but passers-by.[96] This shifts the narrative to justifying LFR on its merits and appears to set expectations about effectiveness of the technology. As we see in the Bridges case on real-world use, it often has mixed results in realising expectations around actual arrests in deployment.[97] Hence this point may be hard to justify the use of LFR, particularly with concerns around false positives.[98]

The rules also state the need for 'necessary and proportionate safeguards and conditions in relation to use, in particular as regards the temporal, geographical and personal limitation'.[99] This is interesting, as it was a key point of contention in the Bridges case around appropriateness of safeguards and criteria for LFR operating in particular locations. As we saw above, this is picked up in College of Policing guidance.

[91] Art 5(1)(d) AIR.
[92] Unless this is not possible.
[93] Art 5(1)(d)(i) AIR.
[94] Art 5(1)(d)(ii) AIR.
[95] Art 5(1)(d)(iii) AIR:

> the detection, localisation, identification or prosecution of a perpetrator or suspect of a criminal offence referred to in Article 2(2) of Council Framework Decision 2002/584/JHA62[96] *and* punishable in the Member State concerned by a custodial sentence or a detention order for a maximum period of **at least three years**, as determined by the law of that Member State.

[96] Art 5(2)(a) and (b) AIR.
[97] CoA para 26–30.
[98] Law Society of England and Wales, *Algorithms in the Criminal Justice System* (Law Society, 2019) 38.
[99] Art 5(2) AIR.

The inclusion of need for authorisation by a judicial or independent administrative authority would be welcome, particularly as the authority would need to be satisfied use is necessary and proportionate in line with conditions above. It is problematic that authorisation can be bypassed if it is really urgent or be requested after the fact when needed.[100] Thus, this hollows out the benefits of any real oversight if it can ultimately be ignored. In any case, the EU law pushes some responsibility for handling this back to Member States (MS), where requests have to be in accordance with national laws on this. Whilst no longer an EU member, the emerging UK position in College of Policing guidance states the authorizing officer can delegate for deployment down the chain of command when urgent.[101] Similarly, despite this law being an EU Regulation, which seeks to harmonise practices across all MS, the current proposal does provide a caveat allowing MS to pass national laws that permit the use of real-time biometric identification in public spaces for law enforcement.[102] Thus, ultimately it enables live use of AFR, if MS create laws to do this. Whilst the UK is no longer an MS, the Bridges case does highlight the kinds of issues that would need to be addressed in any law governing the use of LFR in the future.

2.3.2. Emotional AI as high-risk AI

We now turn to rules around EAI as High-Risk AI Systems (HRAIS). If we look at the list included in the AIR of high-risk AI systems, it includes discussion around law enforcement use of emotion state sensing in Annex III in the legislation (see footnote 90). This covers two examples, namely:

– '6. Law Enforcement' (b) AI systems intended to be used by law enforcement authorities as polygraphs and similar tools or to detect the *emotional state* of a natural person
– '7. Migration, asylum and border control management.' (a) AI systems intended to be used by competent public authorities as polygraphs and similar tools or to detect the *emotional state* of a natural person.[103]

As LFR can also be integrated with these systems, the AIR deems data-intensive predictive policing[104] and law enforcement profiling[105] are also HRAIS, subject to the same rules.[106] This will challenge officer optimism about integration with existing technologies.

[100] Art 5(3) AIR.
[101] CoP para 1.6.1 i.e. from superintendent down but not lower than inspector.
[102] As per conditions in Art 5 (1)(d),(2), and (3) AIR.
[103] This is included in the Annex II AIR (see above footnote 90) and is an updateable list of applications.
[104] **(g)** AI systems intended to be used for crime analytics regarding natural persons, allowing law enforcement authorities to search complex related and unrelated large data sets available in different data sources or in different data formats in order to identify unknown patterns or discover hidden relationships in the data.
[105] **(e)** AI systems intended to be used by law enforcement authorities for predicting the occurrence or reoccurrence of an *actual or potential criminal offence based on profiling of natural persons* as referred to in Article 3 (4) of Directive (EU) 2016/680 or assessing personality traits and characteristics or past criminal behaviour of natural persons or groups; **(f)** AI systems intended to be used by law enforcement authorities for profiling of natural persons as referred to in Article 3(4) of Directive (EU) 2016/680 in the course of detection, investigation or prosecution of criminal offences.
[106] Of less direct relevance but still pertaining to face it includes: '(**c**) AI systems intended to be used by law enforcement authorities to detect *deep fakes* as referred to in article 52(3)'.

The relevance of being deemed an HRAIS is it introduces a raft of new requirements around design of the system. These are covered in Title III at a high level, these include putting in place mechanisms like automated logs, technical documentation, human oversight systems and data quality governance to increase transparency around how a system works and to audit when things go wrong. To bring out more detail, this includes:

- Art 9 – which requires the establishment and maintenance of a risk management system to identify risks when HRAIS are used as intended and reasonable misuse; including implementing risk mitigation and testing regimes.
- Art 10 – focuses on data and data governance, establishing quality criteria around training, validation and testing data.
- Art 11 – technical documentation drafted before going on market.
- Art 12 – ensure record keeping and automated logs.
- Art 13 – 'their operation is sufficiently transparent to enable users to interpret the system's output and use it appropriately.'
- Art 14 – human oversight via 'appropriate human-machine interface tools'

It also puts obligations on different actors in the AI system supply chain too, from providers and users through to importers and distributors to conduct conformity assessments and ensure their systems comply with these requirements above. As users of HRAIS, which the police would be if using emotion sensing systems provided by AI providers, as per Art 29, they would need to take steps including:

- Ensuring input data is relevant to the purpose[107]
- Monitoring operation of high-risk AI according to instructions of use[108]
- Keeping logs, if logs are under their control[109]
- Conducting a DPIA as per Art 35 – using information from Art 13 around transparency information they need to provide.

This approach seeks to increase responsibility at each point in the life cycle and supply chain of HRAIS and not allow the police as users to pass responsibility to the AI provider (e.g. NEC for SWP use of AFR Locate). When we consider the issues faced in the Bridges case around police procurement of LFR as users from the provider NEC, there were questions about adequate human oversight. Art 17 AIR states the requirements for quality management systems that AI providers need to put in place. This is alongside a range of other obligations in Arts 16-23 around HRAIS, such as ensuring it has undergone a conformity assessment. Cummulatively, these measures for HRAIS show how organisations providing AI tools to the police would need to provide more transparency mechanisms around how their system functions before being able to deploy it. With face-based EAI, debate remains around the baseline accuracy of emotion detection technologies, the underlying models of universal emotion, and cross-cultural dimensions of facial expression.[110] This will include determining what appropriate metrics of transparency

[107]Art 29 (3) AIR.
[108]Art 29 (4) AIR.
[109]Art 29 (5) AIR.
[110]McStay and Urquhart (n 16).

will be needed for police use of EAI, if these systems are ever to be deployed operationally.

The UK experience with the Bridges cases and emerging EU policy on regulating AI showcase the types of legal requirements that police need to attend to for future uses of AI and IFS. These are important barriers and safeguards to attend to, particularly in light of optimism shared in Section 2.1 by police officers, as they envision future uses of LFR integrated with other IFS tools. It will be harder for the state to bypass legal controls by outsourcing surveillance roles to private actors, as can occur now,[111] because this legislation targets the whole supply chain. To conclude part 2, whilst the EU direction of travel suggests greater regulation of LFR, and prohibition as the default, in the UK, College of Policing guidance appears more permissive. Despite the guidance seeking to harmonise policing practice across the UK as a national document to ensure consistency, providing public reassurance and guidance for forces, there remain concerns that align with the current scepticism indicated by our officers. In part 3 we provide reflections on police use of IFS in the future.

Part III – concluding reflections on future IFS

In this final section, we formulate lessons from our empirical and legal analysis, framing these as considerations for future IFS, drawing together our thoughts on LFR and EAI. Before doing this, we reiterate what the 7 main contributions of this paper are. Firstly, it provides empirical insights from frontline police officers around the prospective uses of LFR in policing practice. This is unique as it engages at the operational, as opposed to the strategic level, and addresses the gap in qualitative studies with practitioners on this topic. Secondly, it explores present-day scepticism of LFR presented by police officers and contextualises this within current debates around LFR. Thirdly, it explores future optimism about the use of LFR by police officers and how the legal landscape will shape that in practice. To do this, we present the emerging legal landscape around IFS both currently with the Bridges case in the UK, and in the future with the new EU AIR. Fourthly, we anticipate wider risks for future IFS like EAI based on current understandings of LFR. Fifthly, it provides an interdisciplinary approach fusing legal, technical and criminological perspectives to assess the practice and legal requirements around IFS technologies. Sixthly, we argue that the future for IFS will be increasingly regulated, impacting policing practice, and challenging optimism about future uses. Lastly, we have formulated a series of lessons to guide future discussions around IFS, and we now provide these below.

Lesson 1. We urge caution with institutional optimism around future IFS, especially due to the harms arising from *automating suspicion* through biometric technologies. There is a risk of further entrenching bio-deterministic framings of criminality, based on facial data, and this is a harmful precedent to set. Emotional AI in policing poses a particular risk here for future IFS, given it could build on the history of physiognomy, phrenology and Lombrosian rhetoric around reading bodies and criminal intent.

Lesson 2. Innovative uses and resulting legal test cases can establish guidelines for IFS *after* deployment. This occurred with Bridges and provided police with a roadmap. But from a legal perspective, and as an entity of the state, higher standards are needed for law enforcement use of experimental IFS technologies *before* they are deployed. The

[111]Kirstie Ball and Laureen Snider, *The Surveillance-Industrial Complex: A Political Economy of Surveillance* (Springer, 2013).

risks for equality, privacy, discrimination and human rights are too significant to only rely on responsive governance. Instead, guidance for police needs to be more precautionary and prescriptive in guiding behaviour prior to harm occurring. This will also be key for ensuring the suitable *quality of law* exists to protect citizens, as required by human rights law.

Lesson 3. There is significant work to be done in navigating how to *build organisational and technical safeguards* into emerging IFS. For example, more transparency is needed around the *organisational* aspects of specifications formation by law enforcement agencies. What should police learn from experiences with training data and oversight with LFR for procurement processes? Beyond this, how can regulation be baked into the system to add another layer of protection to citizens through *technical* architecture. This is an area needing increased research from technologists in conjunction with policymakers, especially as the law increasingly pushes in this direction, e.g. with the AIR stipulating design requirements for data quality for HRAIS. However, requiring safeguards is one thing; implementing and operationalising them is another.

Lesson 4. IFS, such as EAI, may be integrated with other existing surveillance technologies, and act as a *layer that augments* their functionality. We already see this emerging, as limitations in facial action coding (FACS) means EAI systems increasingly need supplementary information from on body and environmental sensing. This is in order to construct a clearer picture of the subject's emotional state through the use of location, heart rate, temperature, accelerometer data that provides 'context'. Another example could be within IFS systems where with LFR, the addition of EAI could provide further *intent-based information* to complement *identification based information*. So, police could understand not just who this individual is but how they are feeling in the moment. This heightens the risks to citizens' rights and needs a clear appreciation of how integration might pose further harms.

Lesson 5. *Less intrusive techniques* should be used by law enforcement where they can serve the same purpose as IFS, e.g. fingerprinting for identification which provides the same outcome, albeit it cannot be used remotely. This could also help with resource management in law enforcement agencies and address the allure of technological solutionism by avoiding investing in unreliable new IFS.

Lesson 6. It is important to develop *participatory approaches* to involve *operational users* from law enforcement in discussions of deploying new technologies. Their situated experience and sceptical narrative around the value and practical challenges of using new policing technologies can counteract unfounded optimism from the strategic level. The public has to be part of discussions around development and deployment of IFS too. This is especially for *marginalised publics* who face additional equality and fundamental rights risks due to protected characteristics such as gender, race and vulnerability being implicated in IFS, e.g. through disability or age. Further, EAI can create new categories of suspicion and risk, for example through facial micro expressions and inferences about if someone is angry or sad.

Lesson 7. *Effectiveness of IFS* remains a difficult topic. On the one hand, if systems are more accurate, then there are privacy and fundamental rights implications because they enable more invasive surveillance practices. But similarly, if they are less accurate, there are risks of false positives that disproportionality impact those who are more vulnerable. Future IFS, like EAI, have further effectiveness issues, due to the lack of accuracy of models of baseline emotions. In a law enforcement context, this could impact processes

of evidence gathering and admissibility in court, further questioning the utility of such technologies in the long term.

Lesson 8. Law enforcement needs to find mechanisms to *exert control over private vendors* of IFS to increase accountability within this public/private AI supply chain. A key area is oversight of training data processes. IFS vendors may have developed systems in different regulatory, cultural and ethical contexts, but these could cause harms when implemented in a different geographic domain. Thus, despite power asymmetries between vendors and law enforcement, there needs to be verification that the system they are using adheres to fundamental rights commitments. It is key that given the risks from IFS, any balance of interests of citizens with policing goals of prevention, detection and prosecution of crime are not skewed to the latter. The EU AIR is a positive force for improving audibility around the AI supply chain. However, in the UK, the impact this might have is unclear due to Brexit, and the UK College of Policing Guidance indicates a divergence for LFR, which may be mirrored for future IFS too.

Lesson 9. Provenance of images in training data for IFS is a key area of concern. As law enforcement is an arm of the state, it should be held to higher standards around how it sources images for IFS. Emerging guidance on LFR, e.g. from the UK College of Policing, indicates social media data could be used for this purpose legitimately. Firms are already marketing access to face datasets for LFR in other parts of the world, e.g. scandal around Clearview in policing in the US.[112] In the same way curation of watchlists for LFR is subject to greater scrutiny, the sourcing of non-police originating images needs better oversight. Risks from police use of social media intelligence have been discussed in different contexts, e.g. in implicating technology firms in outsourced surveillance in the Snowden Revelations or policing UK Riots in 2011. There need to be publicly available guidelines for law enforcement that document how they should handle provenance tracking of images for IFS, particularly as this practice is likely to be covert. This could include embedding metadata into images flagging their origin, lawful basis for collection, use restrictions and what other agencies these can be shared with.

Lesson 10. Law enforcement needs to be responsive to *emergent societal harms and risks*, particularly around integration of IFS with other technologies, e.g. predpol, sentencing systems. Whilst processes like impact assessments are used for initial deployment and help map initial issues, forecasting new harms during deployment needs to be an ongoing focus. Improving horizon scanning for inequalities would be one element, particularly for EAI, e.g. those who display emotion in different ways. This will be needed in addition to process led safeguards like public sector equality duties to ensure any use of new IFS is proportionate, legally compliant and trusted by the public.

Acknowledgements

Thanks to our participants and Prof Andrew McStay for his valuable comments on an earlier draft.

Disclosure statement

No potential conflict of interest was reported by the author(s).

[112]Tate Ryan-Mosley, 'The NYPD Used a Controversial Facial Recognition Tool. Here's What You Need to Know' (2021) MIT Technoloogy Review <https://www.technologyreview.com/2021/04/09/1022240/clearview-ai-nypd-emails/>.

Funding

This work was supported by the Economic and Social Research Council: [Grant Number ES/T00696X/1]; Engineering and Physical Sciences Research Council: [Grant Number EP/V026607/1]; Keele University: [Grant Number Research Strategy Fund].