The **Human Rights, Big Data and Technology** Project

Independent Report on the London Metropolitan Police Service's Trial of Live Facial Recognition Technology

Authors: Professor Pete Fussey & Dr. Daragh Murray

July 2019

E·S·R·C ECONOMIC & SOCIAL RESEARCH COUNCIL

Human Rights Centre | University of Essex

Table of Contents

Acknowledgments

The authors would like to express sincere gratitude to those whose thoughts and insights have informed this report and the thinking behind it. Many of these people were formally engaged in the research while others offered expert opinion. These include: Patrick Grover (National Institute of Standards and Technology, US Department of Commerce), Simon McKay (The Chambers of Simon McKay), Tony Porter (Surveillance Camera Commissioner), Anne Russell (Information Commissioner's Office), Prof. Paul Wiles (Biometrics Commissioner), Lucy Bradshaw-Murrow (Office of the Biometrics Commissioner), Silkie Carlo (Director of Big Brother Watch), Hannah Couchman (Liberty), Sam Dubberley (Amnesty International), Prof. Alexa Koenig (University of California, Berkeley), Prof. Geoff Gilbert (University of Essex) and Prof. Maurice Sunkin QC (University of Essex).

The authors would also like to thank Beverley Brown for her additional research and editorial assistance in compiling this work.

The authors would like to thank those involved in the MPS' trial of live facial recognition technology for their willingness to engage in the research process that resulted in this report. In particular, the authors appreciate their openness and their respect for the independent nature of the research.

Unless indicated otherwise, all opinions are authors' own, as are any shortcomings in the report.

Executive Summary

Overview

Between 2016 and 2019 the Metropolitan Police Service (MPS) conducted a total of 10 test deployments, trialling live facial recognition (LFR) technology during policing operations. This research was initiated in order to provide an independent academic report on this process. Researchers observed the final six test deployments, beginning in Stratford (Westfield) in June 2018. Researchers joined officers on location in the LFR control rooms, engaged with officers responding on the ground, and attended briefing and de-briefing sessions in addition to planning meetings. A number of legal and other documents prepared by the MPS were also reviewed.

This report is focused on issues arising in relation to the MPS' LFR test deployments. It does not directly engage with broader issues regarding the legality, or use, of LFR technology by law enforcement agencies. As such, although certain elements of the analysis presented herein may be relevant to future debates, no conclusions are drawn in that regard.

This report centres on the overall governance of the LFR test deployments, the procedures and practices of LFR in operational settings (as observed over the course of the test deployments), and human rights compliance. A draft of this report was submitted to the MPS so that any factual errors could be noted, and to provide a right of reply. After review of the document, the MPS chose not to exercise this right. This report is independent, was externally funded as part of the ESRC Human Rights, Big Data & Technology Project, and the findings and opinions expressed are those of the authors alone.

Human rights law requires that any interference with individuals' rights be in accordance with the law, pursue a legitimate aim, and be 'necessary in a democratic society'.

As detailed in the report, it is highly possible that the LFR trial process adopted by the MPS would be held unlawful if challenged before the courts. In particular, this report concludes that the implicit legal authorisation claimed by the MPS for the use of LFR - coupled with the absence of publicly available, clear, online guidance - is likely inadequate when compared with the 'in accordance with the law' requirement established under human rights law. This demonstrates a need to reform how the trialling or incorporation of new technology and policing practices is approached by the MPS, and underlines the need for the effective incorporation of human rights considerations into all stages of the MPS' decision making process, including with respect to if, and how, trials should be undertaken. It also highlights a need for meaningful engagement with, and debate on, these issues at a national level.

The report highlights a number of issues arising from the LFR test deployments, and raises some significant concerns. These concerns are most notable with respect to:

> (1) The research process adopted by the MPS to trial LFR technology. The test deployments offered an opportunity to both examine technical accuracy and to understand the implications of LFR on police operations. However, MPS trial methodology focused primarily on the technical aspects of the trials. There is less clarity on how the test deployments were intended to satisfy the non-technical objectives, such as those relating to the utility of LFR as a policing tool. This report raises concerns that the process adopted by the MPS was inadequate with respect to addressing the non-technical objectives identified.
> (2) The absence of an explicit legal basis for the use of LFR, and concerns that the implicit legal basis identified by the MPS is inadequate in relation to the 'in accordance with the law' requirement established by human rights law. This is compounded by the absence of online guidance capable of addressing the 'foreseeability' of how LFR technology was utilised. Without explicit legal authorisation in domestic law, it is highly possible that police deployment of LFR technology may be held unlawful if challenged before the courts;
> (3) Human rights law requires that any rights interference be 'necessary in a democratic society'. MPS analysis did not effectively address this requirement, and it is considered highly possible that the MPS' test deployments of LFR technology would not be regarded as 'necessary in a democratic society' if challenged before the courts; and
> (4) Operational factors relating to inconsistency in the adjudication process, including a presumption to intervene, problems with how the MPS engaged with individuals, and difficulties in obtaining the consent of those affected.

Research Methodology Adopted for the Report

Six test deployments were observed from beginning to end. Observations extended to attendance at pre-deployment police briefings for each test deployment and post-deployment debriefings which usually took place the following day. Observation mainly focused on the operational practices of the intelligence units in the control room: that is, the activities of officers monitoring LFR camera feeds, deliberating over computer-generated matches and, when deemed appropriate, issuing instructions to intercept matched persons. Research also engaged street-based intervention teams responsible for intercepting individuals matched to watchlists by the LFR system, plain clothes officers deployed at the test sites, and uniformed

officers involved in LFR-related public facing activities. Researchers were also invited to several LFR planning meetings.

All documents provided by the MPS were examined. A variety of interview techniques were used to gain additional data. Observations involved detailed conversations with a wide range of MPS staff. These included operational officers, individuals holding tactical and strategic roles, and those engaged in the technical evaluation of LFR. Formal interviews were also conducted with a number of key external stakeholders including oversight bodies, technology evaluation specialists and civil society organisations.

The Nature of the Test Deployments Undertaken by the MPS, and Appropriateness of the Trial Methodology Adopted

Numerous voices, including the Surveillance Camera Commissioner and the Biometrics Commissioner, have stressed the importance of trialling emergent technologies. Several attempts have been made to offer principles to guide this process, yet their development has been piecemeal and no agreed national standards or established oversight mechanisms exist. It is within this context that the MPS trials of LFR took place.

The MPS' trial methodology focused primarily on technical aspects, examining the performance of the technology in live settings. There did not appear to be a clearly defined research plan that set out how the test deployments were intended to satisfy the non-technical objectives, such as those relating to the utility of LFR as a policing tool. This necessarily complicated the trial process, and affected its effectiveness and overall utility.

It is unclear if alternative approaches to testing LFR were considered and discarded. It is uncertain whether the initial decision to trial LFR considered the use of simulated conditions, with volunteer-based watchlists (as adopted in Berlin) or live condition trials focused on technical performance but not policing responses (as in the United States).

The mixing of trials with operational deployments raises a number of issues including with respect to consent, public legitimacy and trust. A key concern is the lack of a clear distinction between research objectives regarding the trial of LFR technology, and the policing objectives associated with operational deployments. This holds particular meaning when considering differences between an individual's consent to participate in research and their consent to the use of technology for police operations. For example, from the perspective of research ethics, someone avoiding the cameras is an indication that they are exercising their entitlement not to be part of a particular trial or are protecting their own right to privacy. From a

policing perspective, this same behaviour may acquire a different meaning and serve as an indicator of suspicion.

This resulted in a number of issues relating to how police officers engaged with individuals on the ground.

The absence of national leadership at government level – including a lack of clear lines of responsibility regarding whether trials should be conducted, and if so how – leaves police evaluation teams with the enormous task of not only undertaking scientific evaluation, but also compensating for a lack of national leadership by recreating and reinterpreting policy anew. While this tension may apply to other trials of police equipment, it is particularly acute in the case of LFR given its intrusive nature, and requires urgent attention for future testing of this technology (as well as other technological innovations). A key element in this regard must be considering and building in human rights compliance from the outset of any trial process, including with respect to if, and how, any trials should be undertaken.

The Legal Basis Underpinning the MPS' Use of LFR

No explicit legal basis exists authorising the MPS' use of LFR technology.

The legal mandate documents prepared by the MPS reference a number of different sources of law, including the common law, the Human Rights Act 1998, the Freedom of Information Act 2000, the Protection of Freedoms Act 2012, the Data Protection Act 2018, and the Regulation of Investigatory Powers Act 2000. Of these, only the common law and the Protection of Freedoms Act 2012 could potentially establish an implicit legal basis for LFR. The other sources either relate to public access to information regarding police activity or regulate the use of LFR technology, without establishing explicit legal authorisation for LFR as such.

The difficulty with relying upon the common law or the Protection of Freedoms Act 2012 as sources of implicit legal authorisation vis-à-vis the use of LFR technology is the ambiguity that will inevitably arise. The 'in accordance with the law' test established under human rights law incorporates a number of different elements, relating both to the existence of a legal basis and the quality of that legal basis. Key in this regard is protection against arbitrary rights interferences, and foreseeability with respect to how the law will be applied.

Existing case law reinforces the concern that the legal basis identified by the MPS may be overly ambiguous. Issues in this regard are discussed in greater detail in Section 3.2. of the report. Similar concerns regarding the absence of a clear legal basis have been raised by Liberty and Big Brother Watch when interviewed for this report, and in academic commentary.

Ultimately, this report concludes that the implicit legal authorisation claimed by the MPS for the use of LFR appears inadequate when compared with the 'in accordance with the law' requirement established under human rights law. The absence of publicly available guidance clearly circumscribing its circumstances of use – thereby facilitating foreseeability – reinforces this point. Without explicit legal authorisation in domestic law it is highly possible that police deployment of LFR technology – as a particularly invasive surveillance technology directly affecting a number of human rights protections, including those relevant to democratic participation – may be held unlawful if challenged before the courts.

The Absence of Effective Analysis Addressing the 'Necessity in a Democratic Society' Determination for LFR

Determining the necessity in a democratic society of any measure that interferences with human rights protections is essential in order to ensure overall rights compliance. In this context this requirement is intended to ensure that measures useful to the protection of public order and the prevention of crime do not inappropriately undermine other rights, including those necessary to the effective functioning of a democratic society, such as the right to private life, the right to freedom of expression, and/or the right to freedom of assembly and association. The test itself involves a number of different elements. An interference will be considered necessary in a democratic society 'if it answers to a "pressing social need", if it is proportionate to the legitimate aim pursued and if the reasons adduced by the national authorities to justify it are relevant and sufficient.'

In order to determine whether LFR is 'necessary in a democratic society' in the circumstances of the MPS' test deployments, impact or risk assessments should be conducted prior to deployment in order to identify and understand any potential human rights harm. This conclusion is supported by the Surveillance Camera Commissioner's recent guidance on 'Police Use of Automated Facial Recognition Technology with Surveillance Camera Systems'.

The MPS did prepare a number of impact/risk assessment documents. However, these documents are regarded as inadequate with respect to engagement with human rights law requirements.

No MPS documents have been seen that clearly set out the justification underpinning the deployment of LFR technology in a manner capable of addressing whether such deployments may be considered 'necessary in a democratic society'. Of particular concern is the lack of effective consideration of alternative measures, the absence of clear criteria for inclusion on the watchlist, including with respect to the seriousness of the underlying offence, and the failure to conduct an effective

necessity and proportionality analysis. For these reasons, and as discussed in greater detail in Sections 3.3.1. and 3.3.2., it is highly possible that the MPS' test deployments of LFR technology would not be regarded as 'necessary in a democratic society' if challenged before the courts.

Operational Factors

Alerts

Overall, the LFR system generated 46 matches over the course of observed test deployments, involving 45 separate individuals. 42 matches were deemed eligible for analysis.

Adjudicating officers judged 16 (38.1%) of these 42 computer generated matches to be 'non-credible'; that is, officers did not believe the image recorded by the LFR technology match the image on the watchlist. MPS officers considered the LFR match sufficiently credible to stop individuals and perform an identity check on 26 occasions. Four of these attempted interventions were unsuccessful, as individuals were lost in the crowd.

Of the remaining 22 stops, 14 (63.64%) were verified as incorrect matches following an identity check. Eight (36.36%) were verified as correct matches following an identity check. This means that across all six observed trials, and from all computer-generated alerts, face recognition matches were verifiably correct on eight occasions (eight of 42 matches, 19.05%).

Watchlist Construction

The condition of being 'wanted' was consistently stated as a criterion for being enrolled on a watchlist. However, ambiguity exists regarding the definition of 'wanted' adopted by the MPS, and documentation indicates that this included both 'wanted by the courts' and 'wanted by the police'. Those included on the watchlist thus apparently ranged from individuals wanted by the courts to those wanted for questioning, across a range of different offences. Discernible differences in meaning and external judicial scrutiny exist between these different categories of 'wanted' persons. Moreover, the identification of 'individuals shown as wanted by the police and the courts' was not the only watchlist criterion in use. MPS documentation also highlighted the use of LFR to identify individuals who present a risk of harm to themselves and others; support ongoing policing activity with regards to a specific problem or location; and assist police in identifying individuals who may be 'at risk or vulnerable'.

The category of 'wanted' (re 'to identify individuals shown as wanted by the police and the courts') was relied on in creating watchlists for all observed test deployments. Refinements to the threshold for inclusion under this criterion were

made from December 2018 onwards. Nonetheless, significant ambiguity remains regarding the criteria used for watchlist construction. This directly affects the 'foreseeability' of MPS activity regarding the use of LFR technology.

The size of the watchlists varied considerably across the observed test deployments. No discernible direct relationship existed between the watchlist size and number of alerts.

Watchlist Accuracy

Legacy data handling systems meant data relevant to watchlists was spread across different databases and each watchlist entry needed to be assembled by manually extracting and merging records from each of these locations. Ensuring accurate and up-to-date information from across these different data sources posed a significant challenge. Such difficulties made compliance with overall standards of good practice complex and placed a significant burden on officers.

Issues to do with the accuracy of the watchlist played out when individuals were stopped on the basis of outdated information. On occasion, individuals were flagged by the LFR technology in relation to a serious offence, but this had already been dealt with by the criminal justice system. However, they were wanted in relation to more minor offences and were arrested accordingly. It is unlikely this lesser offence would have been sufficiently serious to be included in the initial watchlist. This raises additional concerns when LFR is deployed on a necessity calculation intended to address serious crime but is then also used for more minor offences.

Matching Intelligence to LFR Deployments

Police uses of surveillance measures are directed towards protecting the public from crime and upholding public order. However, the legitimacy of any measure must still be determined in relation to the 'necessary in a democratic society' requirement. One key element when evaluating issues of necessity and, by extension, proportionality, is a consideration of the stated purpose of LFR test deployments and, crucially, analysis of the extent to which the use of the technology is 'rationally connected' to this purpose. Most ethical guidance, and legal and oversight provisions governing surveillance also require a clearly prescribed application.

In the first test deployments observed (Stratford), LFR use was regularly justified in briefings on the basis of several perceived benefits including detection, deterrence, intentional crime displacement and disruption. These applications involve clear differences in the purpose of LFR, requiring distinct necessity calculations.

Public Consent

The role of public consent constituted a contentious debate surrounding the LFR test deployments. Like CCTV, LFR is classified by the MPS as a form of overt surveillance and the consent of affected individuals is seen as fundamental. The importance of consent is also emphasised in regulatory instruments. Measures undertaken by the MPS that bear on consent overlapped with attempts to promote public reassurance and to test public opinion.

For consent to be meaningful, several conditions are important:

1. **Informed consent.** The MPS pursued a number of strategies intended to ensure that public consent for LFR constituted informed consent, including the use of uniformed officers to explain the role of the technology to the public, leafleting and signage boards. A key question emerges over the degree to which consent can be considered informed on the basis of the information supplied by the MPS. Information provided transparency regarding the time and location of the LFR test deployments yet less clarity over the purpose of the deployment, who was likely to be the subject of surveillance, and how additional information could be ascertained. With the exception of the morning of the first Soho trial an individual reading or standing next to a sign was out of camera range for each LFR deployment.
   A key conclusion is the importance of being clear about why information is provided to the public. What might be appropriate in respect to issues of public support is not necessarily sufficient or well targeted enough to support individual consent. During test deployments individuals were required to make an informed decision regarding consent in a very short time-frame, a factor exacerbated by the limits on prior knowledge amongst the public.
2. **Consent and opportunities to exercise a different choice.** Opportunities for pedestrians to bypass the cameras and continue walking towards the same destination varied across the test deployments. These ranged from simply crossing the street to a walking detour of an additional 18 minutes to reach the same point.
3. **Capacity to refuse or withdraw consent without penalty.** Treating LFR camera avoidance as suspicious behaviour undermines the premise of informed consent. In addition, the arrest of LFR camera avoiding individuals for more minor offences than those used to justify the test deployments raise clear issues regarding the extension of police powers and of 'surveillance creep'.

These issues highlight the distinctions between gaining consent for research (e.g. trials) and consent for police operations, and the tensions that will inevitably arise during live test deployments.

The Adjudication Process

All observed officer briefings were clear on the importance of human discretion in the LFR process. Officers were consistently instructed that a computer derived match was not sufficient to confirm an identity in and of itself. This is appropriate given the significant error rates associated with LFR and legal stipulations concerning meaningful human intervention in digital decision-making processes.

Adjudication practices varied across the deployments. These can be placed within three distinct categories:

1. **Multiple adjudicators in the control room**. Multiple operators brought additional scrutiny to the process but also raised the likelihood of contrasting approaches within the same adjudication team.
2. **Simultaneous adjudication and street engagement**. This involved intelligence officers radioing through a description of a LFR match while they were still in the process of deliberating over the credibility of the alerted match. A decision to trigger the street intervention team to start looking for the matched individual may have sound operational reasons. However, every instance in which this simultaneous approach was followed led to an attempt to engage a matched individual. This forms part of a wider and discernible 'presumption to intervene'. Greater clarity is possible over whether communications to intervention teams are instructions to maintain observation or an instruction to intervene.
3. **Mobile devices and simultaneous adjudication on the street and in the control room.** During the second Romford test deployment, the decisive choice to intervene with a matched individual was made by street-based officers equipped with handheld devices capable of receiving LFR alerts on at least five occasions. Decisions of the control room-based intelligence teams to engage a subject were never rejected by mobile-equipped officers. Decisions by the control room-based intelligence units not to intervene were frequently 'overruled' by street-based mobile-equipped officers on the basis of their separate access to imaging information. These processes also contribute towards a presumption to intervene.

Physical Factors Relating to Deployments

The physical characteristics of a particular area, along with the spatial location of intervening officers, had significant bearing on the adjudication process and subsequent street intervention. The spatial deployment of officers to provide the best opportunity to locate a matched individual on the street constricted the time available to adjudicators to reach a decision. Conversely, situating officers further from cameras afforded more time for control room adjudication but increased the likelihood of losing track of individuals.

1. Introduction

This report is authored by Professor Pete Fussey,[1] and Dr. Daragh Murray,[2] members of the ESRC Human Rights, Big Data & Technology Project, based at the University of Essex Human Rights Centre.[3] Prof. Fussey and Dr. Murray engaged in an agreed schedule of research to produce an independent academic report covering the final six of ten live facial recognition test deployments undertaken by the Metropolitan Police Service (MPS). The focus of engagement with the MPS covered human rights compliance, overall governance issues, and the operational uses of live facial recognition (LFR) technology over the course of the test deployments. This report is the product of that research. A draft of the report was submitted to the MPS so that any factual errors could be noted, and to provide an informed right of reply. After reviewing the document, the MPS chose not to exercise their right of reply. Relevant sections of the right to reply are cross referenced in the main report where appropriate. This report is independent, was externally funded,[4] and the findings and opinions expressed are those of the authors alone.

This report is focused on issues arising in relation to the MPS' LFR test deployments. It does not directly engage with broader issues regarding the legality, or use, of LFR technology by law enforcement agencies. As such, although certain of the analysis presented herein may be relevant to future debates no conclusions are drawn in that regard.

The authors wish to highlight the engagement with this research project demonstrated by the members of the MPS involved in the LFR test deployments.[5] They were consistently professional, open with information and in their engagement with the research process, and fully respected the independent nature of this research. Relevant documents were produced, access was granted to key meetings during the course of the observation period, and no obstacles were encountered in accessing any sites or individuals.

---

[1] Prof. Pete Fussey is based at the Department of Sociology, University of Essex, and is Deputy Director of the Human Rights, Big Data & Technology Project.

[2] Dr. Daragh Murray is a Senior Lecturer in the School of Law & Human Rights Centre, University of Essex, and a Deputy Workstream Director on the Human Rights, Big Data & Technology Project.

[3] For more information on the Human Rights, Big Data & Technology project, please see www.hrbdt.ac.uk. The Human Rights, Big Data & Technology project is funded by the UK Economic and Social Research Council (ESRC), the source of financial backing for this report and its underpinning research

[4] See footnote 3. Different funding models have driven the commission of LFR trials. In London the MPS internally funded the deployments of LFR technology. The other major public UK trials of LFR were conducted by South Wales Police between May 2017 and March 2018. This scheme was majority funded by the Home Office under the Police Transformation Fund with the condition of commissioning an independent evaluation built into the resource allocation.

[5] The term 'test deployments' is used in this report as LFR testing occurred during live operational deployments, and were influenced by the reality of those deployments. As such, use of the term 'trial' appeared inappropriate.

A total of 10 LFR test deployments were conducted by the MPS between 2016 and 2019. An additional non-operational trial was conducted in April 2019. The sequence of test deployments was as follows:

- Notting Hill Carnival, 28-29 August 2016
- Notting Hill Carnival, 27-28 August 2017
- Remembrance Sunday Commemorations, Whitehall, 12 November 2017
- Port of Hull docks, assisting Humberside Police, 13-14 June 2018
- Stratford (Westfield), London, 28 June 2018
- Stratford (Westfield), London, 26 July 2018
- Soho (Cambridge Circus and Leicester Square), 17 December 2018
- Soho (Leicester Square), 18 December 2018
- Romford (Town Centre), 31 January 2019
- Romford (Town Centre), 14 February 2019.

The authors of this report observed the final six test deployments, beginning with the first deployment in Stratford (Westfield) in June 2018. Researchers did not observe a non-operational trial conducted in April 2019.

This report highlights a number of issues arising from the LFR test deployments. The report acknowledges the difficulties faced when seeking appropriate use of emerging technologies for the pursuit of public safety in a context where national guidance and leadership is largely absent. The report also notes a number of refinements to the approach adopted by the MPS as the test deployments progressed. However, the report raises some significant concerns. These are most notable with respect to: (a) the research process adopted by the MPS to trial LFR technology, and whether this was capable of addressing the identified objectives; (b) the absence of an explicit legal basis for the use of LFR, and concerns that the implicit legal basis identified by the MPS is inadequate in relation to the 'in accordance with the law' requirement established by human rights law; (c) the absence of effective analysis addressing the 'necessity in a democratic society' of the use of LFR in the circumstances trialled by the MPS, as required by human rights law; and (d) operational factors relating to inconsistency in the adjudication process, a presumption to intervene, problems with how the MPS engaged with individuals, and difficulties in obtaining the consent of those affected.

As detailed in this report, it is highly possible that the LFR trial process adopted by the MPS would be held unlawful if challenged before the courts.[6] This demonstrates

[6] It is noted that, at the time of writing, South Wales Police's trial of LFR is currently being challenged before the courts, indicating the existence of a case to answer with respect to the legality of certain elements of the LFR trial process. Further demonstrating the level of formal scrutiny being applied to this technology, the US House of Representatives Committee on Oversight and Reform held a hearing to examine the use of facial recognition technology by government and commercial entities, its impact on civil rights and liberties, and the need for oversight during the same week (https://oversight.house.gov/legislation/hearings/facial-recognition-technology-part-1-its-impact-on-our-civil-rights-and).

a need to reform how certain issues regarding the trialling or incorporation of new technology and policing practices are approached by the MPS, and underlines the need to effectively incorporate human rights considerations into all stages of the MPS' decision making processes. It also highlights a need for meaningful leadership on these issues at a national level. It is appropriate that issues such as those relating to the use of LFR are subject to scrutiny, and the results of that scrutiny made public. The MPS' willingness to support this research is welcomed.

1.1.Report Methodology

This research was initiated in order to provide an independent academic report on the MPS' final six LFR test deployments, with research commencing in June 2018. The research process has been designed to be distinct from the MPS' own review which focuses on the technical aspects of the process. There has been a dialogue between the authors of the two reports to ensure that any differences in issues of objective fact were addressed in advance and that the same sets of statistics regarding the LFR test deployments were used. The inferences drawn from these facts may differ, however.

1.1.1. Focus of the Report

This report centres on human rights compliance, overall governance of the LFR test deployments, and the procedures and practices of LFR in operational settings (as observed over the course of the test deployments). To gain the necessary coverage of key issues and to provide analysis that was sufficiently detailed three core areas of activity were addressed.[7] First, the pre-deployment planning for observed test deployments was examined with a specific focus on the legal and operational bases for deployment, types of external engagement, the specific case for each deployment, and watchlist construction. As the researchers were not involved in the initial phases of the test deployments, and research was only initiated after the fourth test deployment, the MPS' initial decision to trial LFR, how it was to be trialled, and the legal considerations applicable to the trial process, could not be examined in detail.[8] Second, the physical deployment of LFR and related ethics and human rights issues were examined, incorporating issues such as consent, public information and the technological architecture (e.g. siting of cameras, purpose and parameters of data retention, etc.). Third, the operational setting was studied, focusing on how the technology was used in practice. This was crucial as the potential of LFR technology is dependent on its operational environment. Key considerations here concerned human decision-making in relation to LFR alerts and operator engagement with the technology itself. In line with established qualitative social science methodology sufficient flexibility was built into the research approach to accommodate

[7] This is not to suggest that these are the only areas of interest in relation to LFR.
[8] Issues to do with the legal basis underpinning the trials, and the necessity of LFR, are discussed further in Section 3.2 and 3.3.

unanticipated and previously unforeseeable deployment-related issues that could hold direct relevance for the research.[9]

1.1.2. Sources of Data

This research used established qualitative social science data collection tools to gather the information supporting the analysis presented in this report. In line with research ethics procedures governing research at the University of Essex and appropriate national standards, all contributions by participants are anonymised unless express consent was provided to attribute quotes.

Six test deployments were observed from beginning to end, including briefing and de-briefing sessions.[10] Observation methods drew on proven ethnographic social science techniques recognised as effective for researching complex operational police[11] and surveillance[12] practices. These techniques correspond with methods used by the study most analogous to this one – the independent evaluation of South Wales Police's use of LFR technology.[13] Observations extended to attendance at pre-deployment police briefings for each test deployment and post-deployment debriefings which usually took place the following day. While the test deployments were taking place observation mainly focused on the operational practices of the intelligence units in the control room: that is, the activities of officers monitoring LFR camera feeds, deliberating over computer-generated matches and, when deemed appropriate, issuing instructions to intercept matched persons. Research also engaged street-based intervention teams responsible for intercepting individuals matched to watchlists by the LFR system, plain clothes officers deployed at the test sites, and uniformed officers involved in LFR-related public facing activities. Researchers were also invited to several LFR planning meetings.

In order to conduct the legal analysis all documents provided by the MPS were examined.[14] This was coupled with a review of relevant case law, and an analysis of existing legal literature addressing issues pertinent to LFR. The decision was made to focus primarily on the case law of the European Court of Human Rights.[15] The

[9] For further information on the methodology adopted for the purposes of this report, see Section 1.1.2.
[10] Test deployments were observed by Prof. Pete Fussey who lead the social science research underpinning this report. Dr. Daragh Murray lead the legal analysis. The analysis presented in this report is interconnected, and based on contributions from both authors.
[11] Recognised landmark academic studies of policework using this type of method include Banton, M. (1964) *The policeman in the community*, London: Tavistock; Manning, P. (1977) *Police Work*, Cambridge, MA: MIT Press; Punch, M. (1979) *Policing the Inner City: A Study of Amsterdam's Warmoesstraat*, London: Palgrave Macmillan; Loftus, B. (2012) *Police culture in a changing world*, Oxford: Oxford University Press.
[12] For example, Norris, C., and Armstrong, G. (1999) *The Maximum Surveillance Society*, Oxford: Berg; McCahill, M. (2002) *The Surveillance Web: The rise of visual surveillance in an English city*, Cullompton: Willan; Smith, G.J.D. (2015) *Opening the Black Box: The Work of Watching*, London: Routledge.
[13] Bethan Davies, Martin Innes and Andrew Dawson (2018) *An Evaluation of South Wales Police's Use of Automated Facial Recognition*, Cardiff: Universities' Police Science Institute, Crime and Security Research Institute, Cardiff University.
[14] All documents provided by the MPS are listed in Annex 1.
[15] Reference to other bodies of law, in particular the Court of Justice of the European Union, is made where relevant. The decisions of the Court of Justice of the European Union bind the UK.

longstanding case law of the European Court of Human Rights has significantly developed understandings of the content of relevant rights, and it is likely that should any legal challenges to the use of LFR be presented these will draw heavily upon this case law. In addition, relevant codes of practice, strategy documents, reports, blogs, and other documents from relevant independent and government regulatory bodies with an interest in the use of LFR were drawn upon. The authors are not expert in data protection law and no comment will be made with respect to the data protection law compliance of the test deployments.[16]

A variety of interview techniques were used to gain additional data. Observations involved detailed conversations with a wide range of MPS staff. These included operational officers, individuals holding tactical and strategic roles, and those engaged in the technical evaluation of LFR. The staggered nature of the test deployments meant follow-up conversations were possible so issues could be returned to, facts could be checked and attempts made to address any issues of clarity.

Formal interviews were also conducted with a number of key stakeholders. Representatives from Liberty and Big Brother Watch gave on-the-record interviews for this report. These accounts are important given both organisations were present on the streets at almost all deployments and therefore witnessed many police interactions with those matched to watchlists by LFR technology. These organisations are involved in legal challenges against police uses of LFR, including against the MPS.

The MPS documentation (and website) states that 'The way we use [LFR] is monitored and regulated by' three agencies: the Information Commissioner's Office (ICO), the Surveillance Camera Commissioner, and the Biometrics Commissioner. All three were approached by the authors. The Information Commissioner's Office provided written answers to questions presented by the researchers, the Surveillance Camera Commissioner gave an on-the-record interview and a meeting was held with the Biometrics Commissioner.[17]

In accordance with standard academic practice, additional interviews and discussions with experts were undertaken to gain contextual knowledge of relevant issues. Those interviewed included professional evaluators of face recognition

[16] The Information Commissioner's Office has prepared a guide to law enforcement processing, available at: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/. It is noted that data protection law forms a significant part of Liberty's challenge to South Wales Police's. use of live facial recognition technology. See, *Edward Bridges v. The Chief Constable of South Wales Police and the Secretary of State for the Home Department*, Skeleton Argument ton Behalf of Claimant, High Court of Justice Queen's Bench Division Administrative Court for Wales, CO/4805/2018.

[17] During this meeting the Office of the Biometrics Commissioner stated that, contrary to statements made in the MPS documentation above, monitoring and regulating LFR is not within the Biometrics Commissioner's statutory remit.

technology, academics, legal professionals and individuals occupying specialist roles in the MPS. No request to speak to anyone in the MPS was declined.

1.2. Issues arising in relation to the nature of LFR and how the MPS trials were conducted

1.2.1. What is LFR Technology?

LFR technology allows for the real time biometric processing of video imagery in order to identify particular individuals.[18]

The MPS' LFR trials were conducted on the basis of a series of distinct static deployments, utilising fixed position cameras that were deployed exclusively for the purposes of the test deployments.

During a deployment images obtained by means of a dedicated camera system are streamed in real time to a facial recognition system. This software biometrically processes the images in order to identify any faces, creates a digital signature of identified faces, and then analyses those digital signatures against a database (referred to as the 'watchlist') in order to determine if there are any matches. If a match is identified an alert is generated. This alert is generated in the control room where the software is deployed and monitored in real-time by police officers,[19] and may also be visible on portable devices carried by officers in the area of operation. This alert displays the live image (i.e. the image captured by the LFR camera system) and the image matched from the watchlist, so that a visual comparison can be made before a decision to intervene with an individual is taken.

During the test deployments camera systems were either deployed in fixed locations, similar to traditional street-based surveillance cameras,[20] or on a mobile facial recognition van. Two cameras were typically deployed in order to ensure full coverage of the scene under observation.[21]

According to MPS documentation: digital signatures that did not generate a match were discarded immediately after processing, while those that did generate a match

[18] While open street surveillance cameras constitute an available frame of reference and a natural point of analogy with LFR, it is important to notice the differences and capacity for additional intrusion possessed by the latter. In addition to significantly enhanced data matching, LFR's reliance on biometric processing invests the technology with additional and powerful capabilities. This point is recognised both by the Surveillance Camera Commissioner (Surveillance Camera Commissioner, 'Police Use of Automated Facial Recognition Technology with Surveillance Camera Systems: Section 33 Protection of Freedoms Act 2012', March 2019, p. 2) and the Biometrics Commissioner (e.g. "Any biometric, by definition, will be extremely intrusive as regards individual privacy and, therefore, liberty", House of Commons (2019) *Science and Technology Committee, Oral evidence: Work of the Biometrics Commissioner and the Forensic Science Regulator*).

[19] During the test deployments control rooms were established either in a room close to the area of operations, or in the mobile face recognition van. The term 'control room' is used throughout this report to denote both.

[20] In Stratford, for example, camera systems were attached to poles.

[21] This is discussed in more detail in Section 4.4.1 and 4.8.

were retained for a 30-day period;[22] no database of individuals or their movements was established as a result of the trials; facial recognition software was not run on other camera systems, and no attempt was made to conduct automated analysis on the data produced.

However, potential uses of LFR technology are significantly broader than that observed during the test deployments. For instance, it is possible for LFR software to be integrated into police body worn cameras or city-wide surveillance camera networks, on a 24/7 basis, and for the resultant data to be subject to automated analysis.[23] This would allow, for example, for the creation of a database containing a record of each individuals movements within a city. This database could then be subject to further automated analysis, in order to identify factors such as unusual patterns of movement, participation at specific events, or meetings with particular people. The significant future capability of LFR software was noted by the Surveillance Camera Commissioner:

> overt surveillance is becoming increasingly intrusive on the privacy of citizens; in some case more so than aspects of covert surveillance because of the evolving capabilities of emerging technologies.[24]

Big Brother Watch compared the use of LFR to a large-scale identity check, equivalent to checking papers or fingerprinting at physical checkpoints.[25]

1.2.2. Bias and Discrimination

The issue of potential bias and discrimination has been particularly prominent in current debates regarding LFR technology and represents an area of significant public interest.[26] This report therefore highlights some key elements of the debate, in order to illustrate some of the issues that police forces considering the deployment of LFR technology should take into account.

---

[22] See, for example, Live Facial Recognition, (LFR) Legal Mandate, 23 July 2018, p. 6. A total of 150 alerts were generated across all test deployments, with 46 alerts during the research period. Issues related to data protection and retention periods are discussed further in, 'Data Protection Impact Assessment for the use of Live Facial recognition within the MPS', 25 July 2018.

[23] For a very general overview of how facial recognition technology is used in this manner in China, for example, see, Bernard Marr, 'The Fascinating Ways Facial Recognition AI Are Used In China', *Forbes*, 17 December 2018. See also, Shannon Liao, 'Chinese police are expanding facial recognition sunglasses program', *The Verge*, 12 March 2018. In addition, several technology companies operating in the UK have brought to market mobile body worn cameras equipped with face recognition technology (see among others, https://www.digitalbarriers.com/resources/). The public deployment of LFR continues to attract controversy. In May 2019 San Francisco became the first US city to ban public use of the technology after legislators voted overwhelmingly in favour of the restriction (see D. Lee (2019) 'San Francisco is the first US city to ban facial recognition.' 15th May, https://www.bbc.co.uk/news/technology-48276660).

[24] Surveillance Camera Commissioner, Annual Report 2017-18, p. 35. This quote indicates some of the difficulties associated with classification of LFR technology as overt.

[25] Interview with Silkie Carlo, Director, Big Brother Watch.

[26] Human rights considerations concerning the prohibition of discrimination are discussed further below in Section 2.1.3.

First, debate has been generated over whether LFR technology may be deployed in a manner that gives rise to discrimination concerns.[27] This is analogous to traditional concerns associated with potentially discriminatory policing practices,[28] and – applied to LFR - may depend on factors such as input data and watchlist composition, or the nature of the deployment. Second, concerns have been raised regarding bias built into LFR technology. This means that the technology may behave differently depending upon an individual's sex, race, or colour, thereby giving rise to discrimination.

Assessing the relationship between LFR technology and bias is complex. Part of this complexity lies in the way that the phrase 'facial recognition' is used to describe a diverse range of activities which may not be generalisable. For example, strong performance in one application, such as matching standardised images taken in controlled lighting conditions, may not translate to other applications, such as identifying faces in social media video or live streams. Equally, existing evaluations point to highly varied performance between different commercial algorithms.[29] Without a clear understanding of whether claims are being made based on tests for similar tools, applications, or purposes, caution is required when considering LFR performance. Different algorithms and different applications assert biases in different ways, and therefore require analysis on an application-by-application basis.

Definitive independent evaluation of face recognition technology performance is limited, and it is difficult to make categorical claims on the subject. However, some recourse to independent technical evaluation is possible. Since the 1990s the National Institute of Standards and Technology (NIST), part of the US Federal Department of Commerce, has provided technical evaluation of face recognition algorithms. These evaluations have been collected in various reports and most comprehensively in the periodic 'Face Recognition Vendor Test (FRVT)'. The latest iteration of this test (2018) assessed 127 commercially available face recognition algorithms on a bank over 24 million images.

The NIST tests reveal varied performance of face recognition algorithms across age, gender and ethnicity. Variations in performance appear to be amplified when these three variables are combined. For example, the most recent NIST Face Recognition Vendor Test concluded that face recognition performance on static images declines

[27] For example, Big Brother Watch (2018) *Face Off: The lawless growth of facial recognition in UK policing*, London: Big Brother Watch. Available at: https://bigbrotherwatch.org.uk/wp-content/uploads/2018/05/Face-Off-final-digital-1.pdf.

[28] For example, The Lammy Review (2017) *An independent review into the treatment of, and outcomes for, Black, Asian and Minority Ethnic individuals in the Criminal Justice System*, available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/643001/lammy-review-final-report.pdf.

[29] NIST (2018) *Ongoing Face Recognition Vendor Test (FRVT) Part 2: Identification*, Washington DC: US Department of Commerce, p.7 Available at: https://doi.org/10.6028/NIST.IR.8238. This is also a reversal of findings from earlier Face Recognition Vendor Tests, e.g. from NIST (2014) *Face Recognition Vendor Test (FRVT): Performance of Face Identification Algorithms*, Washington DC: US Department of Commerce. Available at: https://nvlpubs.nist.gov/nistpubs/ir/2014/NIST.IR.8009.pdf.

when reviewing ageing faces.[30] Similar tests of gender classification algorithms highlight a tendency to produce fewer false positives for males, with this gendered effect becoming more pronounced with ageing.[31] Other studies have identified the influence of race in exaggerating gender disparities. For example, research by Buolamwini and Gebru tested three widely used gender classification algorithms and found that "all classifiers performed best for lighter individuals and males overall. The classifiers performed worst for darker females".[32] Research also indicates that the performance of face recognition algorithms is highly varied in relation to ethnicity. Some algorithms are more likely to produce higher numbers of false positives, while others produce higher rates of false negatives.[33] Moreover, technical evaluators have argued that it is important to differentiate matches *between* ethnic groups and matches *within* ethnic groups. A non-biased algorithm would be expected to have similar false positive rates *within* ethnic groups, regardless of which ethic group was under consideration.[34] These disparities in performance may be linked to factors such as difficulties intrinsic to biometric recognition, and inadequate (i.e. insufficiently diverse) training data.

An added dimension of this debate is that, an examination of technical reviews reveals that historically, measures of face recognition capability have largely prioritised overall system performance. Such performance indicators usually exclude demographic neutrality.

---

[30] NIST (2018) *Ongoing Face Recognition Vendor Test (FRVT) Part 2: Identification*, Washington DC: US Department of Commerce, p.7 Available at: https://doi.org/10.6028/NIST.IR.8238. This is also a reversal of findings from earlier Face Recognition Vendor Tests, e.g. from NIST (2014) *Face Recognition Vendor Test (FRVT): Performance of Face Identification Algorithms*, Washington DC: US Department of Commerce, available at: https://nvlpubs.nist.gov/nistpubs/ir/2014/NIST.IR.8009.pdf.

[31] NIST (2015) *Face Recognition Vendor Test (FRVT) Performance of Automated Gender Classification Algorithms*, Washington DC: US Department of Commerce, available at https://nvlpubs.nist.gov/nistpubs/ir/2015/NIST.IR.8052.pdf.

[32] Buolamwini, J., and Gebru, T. (2018) Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification, *Proceedings of Machine Learning Research* 81:1–15, p12. It is important to note that this research has stimulated further debate. This dispute also directly links to the issues outlined above concerning the varied uses and types of algorithms. Amazon, who have developed a face recognition system ('Rekognition') and since sold it to several US law enforcement agencies, argued that the analysis was compromised because the study focused on 'facial analytics' (i.e. gender classification) rather than 'face recognition'. In turn, Buolamwini published a robust and detailed rejoinder to these criticisms. The details of both extend beyond the scope of this report but the Amazon critique can be accessed here: Wood, M. (2019) 'Thoughts on Recent Research Paper and Associated Article on Amazon Rekognition', AWS blog post, https://aws.amazon.com/blogs/machine-learning/thoughts-on-recent-research-paper-and-associated-article-on-amazon-rekognition/. Buolamwini's rejoinder is available here: Buolamwini, J. (2019) 'Response: Racial and Gender bias in Amazon Rekognition—Commercial AI System for Analyzing Faces', *Medium*, 25 January, available from https://medium.com/@Joy.Buolamwini/response-racial-and-gender-bias-in-amazon-rekognition-commercial-ai-system-for-analyzing-faces-a289222eeced.

[33] Background interview with NIST representative (12 March 2019).

[34] There have been further attempts to evaluate these effects. For example, using 'nationality' as a proxy for 'ethnicity', NIST tested the performance of face recognition algorithms *between* ethnic groups by pairing facial images from different countries during 2018 Face Recognition Vendor Test (NIST (2018) *Ongoing Face Recognition Vendor Test (FRVT) Part 1: Verification*, Washington DC: US Department of Commerce, available at https://www.nist.gov/sites/default/files/documents/2018/06/18/report_2018_06_18.pdf). While heavily caveated, the results identify some differences in performance between members of different national groups. Also significant is the finding that false matches are "higher for demographic-matched impostor[s]" (NIST (2018b) *Ongoing Face Recognition Vendor Test (FRVT) Part 1: Verification*, p57-66.). In other words, there is a higher likelihood of being wrongly matched to someone from the same demographic group, than to someone belonging to a different ethnic group. Given that the aforementioned research demonstrates that algorithmic performance varies depending on different demographic groups, some individuals are more likely to be falsely matched by virtue of membership of a particular ethnic group.

The past 12 months have seen the emergence of developers' claims that their products have uniform performance across populations. While many such claims lack discernible independent verification, the increasing prominence of this theme is notable. Moreover, technical experts interviewed for this report have stressed the possibility of additional approaches towards reducing demographic bias, such as the use of complex mathematics to weight various populations in the training data.[35]

The prohibition of discrimination requires that police forces take active measures to ensure that neither the LFR technology nor its means of deployment violate the prohibition of discrimination. To do so, it is incumbent on those using LFR to understand its shortcomings, and the degree to which they affect issues of bias and discrimination.

1.2.3. The Research Process Adopted by the MPS to Trial LFR Technology

The six observed test deployments occurred during live policing operations and primarily involved non-volunteer participants.[36] The previous four test deployments appear to have been run on a similar basis. One further trial was conducted using a watchlist populated solely with volunteers, but this took place after the 10 public test deployments had concluded (April 2019), and lies outside the scope of this report.

It is unclear whether the initial decision to trial LFR considered the use of simulated conditions, with volunteer-based watchlists (as adopted in Berlin[37]) or live condition trials focused on technical performance but not policing responses (as in the evaluations conducted by the United States Federal Government[38]). The MPS has not presented documentation setting out why the initial decision was made to trial LFR technology, why live test deployments in 'natural conditions' were chosen at the outset, or how these test deployments would ensure that research objectives were met.[39] Concerns in this regard have been raised by relevant bodies. For example, the London Policing Ethics Panel noted:

> …if a primary purpose for trialling the [LFR] technology has been simply to ascertain how effectively facial recognition can identify individuals on

[35] Background interview with NIST representative (12 March 2019).
[36] A small number of volunteers were included in each trial for purposes of the technical evaluation.
[37] See, Bundesministerium des Innern [Federal Ministry of the Interior] (2018) *Written answer to Bundestag member Alexander Ulrich*, available at https://andrej-hunko.de/start/download/dokumente/1205-technik-und-hersteller-am-ueberwachungsbahnhof-suedkreuz-mdb-ulrich/file; Deutscher Bundestag (2018) *Schriftliche Fragen mit den in der Woche vom 29. Januar 2018 eingegangenen Antworten der Bundesregierung, 19. Wahlperiode [Written questions received in the week of January 29, 2018 and Responses of the Federal Government, 19th electoral term]*, p7. 02.02.2018, Saarbrücken: Satzweiss, available at http://dipbt.bundestag.de/doc/btd/19/006/1900605.pdf.
[38] NIST (2017) *Face In Video Evaluation (FIVE) Face Recognition of Non-Cooperative Subjects*, Washington DC: US Department of Commerce, available at https://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8173.pdf.
[39] Reflecting on the April 2019 volunteer-only LFR trial, members of the Metropolitan Police Service evaluation team informed researchers that the volunteer-only methodology offered only limited lessons for policing, and that it was difficult to translate findings from this more artificial setting into learning for the operational environment. A key point here, however, is the extent to which considerations are explored in advance of test deployments.

> a watch list in a crowd situation, this could in principle have been achieved in simulated conditions. The technology would then have been tested on people who had consented to participate in a simulation, rather than on the public at large. This could have provided the required baseline data on, for instance, the rate of false positives and false negatives, without involving members of the public in trials associated with police operations.
>
> […]
>
> if the argument is that LFR must be tested in natural conditions, a better justification for trialling it on the public at large would have been that all options for testing and refining it in simulated natural conditions had been exhausted. The MPS has not presented this claim to the public. In consequence, what has been discovered during the MPS operational trials regarding the effectiveness of the technology appears to be of value, but this knowledge has been bought at the price of some public disquiet.[40]

The Biometrics and Forensics Ethics Group also identified problems with testing LFR technology 'in the wild', i.e. during operational deployments. Their remarks apply more generally than to the emphasis on machine learning made here:

> Where machine learning[41] is taking place through the exposure of the algorithm to new sources of data in a public space, every police trial is potentially an operational deployment and every operational deployment is experimental and trial-like. This inherent ambiguity means that it is difficult to discern the purpose of the recent police field trials; were they police operations or experiments? This raises questions about:
>
> - securing consent for 'trial' participation;
> - the nature and composition of the watchlists (whether they should be simulated or contain images of persons of interest); and
> - the extent to which field trials risk undermining public confidence and trust in policing.[42]

[40] London Police Ethics Panel Interim Report on Live Facial Recognition July 2018 p. 9.

[41] Citing Parkhi, O. M., Vedaldi, A., Zisserman, A. (2015) Deep Face Recognition, Visual Geometry Group, University of Oxford, machine learning is defined in this context 'Biometric technologies for facial recognition require machine-learning algorithms that have been trained on a dataset of labelled images' (Biometrics and Forensics Ethics Group Facial Recognition Working Group (2019) Ethical Issues Arising from the Police Use of Live Facial Recognition Technology).

[42] Biometrics and Forensics Ethics Group Facial Recognition Working Group (2019) Ethical Issues Arising from the Police Use of Live Facial Recognition Technology, p. 3.

The mixing of trials with operational deployments thus raises issues of consent and issues of public legitimacy and trust.[43] This point was echoed by the Surveillance Camera Commissioner in an interview for this report:

> I would say that despite having sat on the biometric board, I had never been entirely clear what the range and scope of the pilots have been and I think the lack of clarity on that has undermined its legitimacy because it has been seen as de facto, a policing operation that grows and evolves and not necessarily a pilot and I think that has undermined the trust in the organisations using it. I think that's been one of the key determinants.[44]

Oral evidence given by the Biometrics Commissioner to the House of Commons Science and Technology Committee during March 2019 enlarges on this point, while recognising that the approach adopted by the MPS had demonstrated improvements over the course of the test deployments:[45]

> [automated facial recognition] is the first of a new generation of biometrics whose deployment offers something slightly different from a forensic capability and is technically and scientifically as important to the future of policing as the forensic techniques… [to] work out how you would deploy it, if you were to deploy it, and things like whether it is legal and all the rest of it, you need to conduct a trial…
>
> A slight problem here is that I am not sure my understanding of the word "trial" is always the same as the police service's understanding of it. The police tend to regard trials as something you try before you use it operationally, which is not quite the same. I see the conclusion of a trial as a process when you take a decision on the basis of the evidence you have gathered on whether it is appropriate to go forward…
>
> I would like to see those trials being more consistent in the way they are put together and the methodology that they use both from the point of view of it being good science and because at some point down the line the police will be faced with a whole range of biometrics… I would like

[43] Issues of consent are returned to below in Section 4.4.

[44] Interview with Tony Porter, Surveillance Camera Commissioner.

[45] "I think that in the case of the Metropolitan police it got better, if I may put it that way. When it started, it could have been accused of being slightly haphazard, but as things went along and they brought in external people to help them conduct it the methodology got better", House of Commons (2019) *Science and Technology Committee, Oral evidence: Work of the Biometrics Commissioner and the Forensic Science Regulator*, HC 1970, Tuesday 19 March, transcript available ar http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/science-and-technology-committee/the-work-of-the-biometrics-commissioner-and-the-forensic-science-regulator/oral/98556.html.

> to see more standardisation in the way they go about conducting those trials.[46]

The Biometrics Commissioner (2018) noted that there may be valid reasons for conducting public trials:

> Whilst there is good evidence of the matching capabilities of different facial matching software products in reasonably controlled use environments, such as matching custody images or passports at airports, there is little evidence as yet about matching for this much more challenging use … trials can be justified if they have been carefully designed to provide new evidence to fill these gaps in knowledge and the results of the trials are published and externally peer reviewed.[47]

The Biometrics Commissioner's emphasis on carefully designed trials is, of course, key. Numerous attempts have been made to identify core standards for testing similar initiatives. Perhaps the most widely cited of these methodologies was set out in the Government Chief Scientific Advisor's 2015 report into forensic science.[48] The MPS' LFR technical evaluation team informed the authors of this approach, and reference to these standards was made in several planning meetings.[49] In March 2019 the Surveillance Camera Commissioner released guidance on police uses of LFR technology that adapted this guidance for the explicit purpose of establishing a 'process that should be followed when piloting automatic facial recognition'.[50] This is set out below in Fig 1.1.

---

[46] House of Commons (2019) *Science and Technology Committee, Oral evidence: Work of the Biometrics Commissioner and the Forensic Science Regulator.*

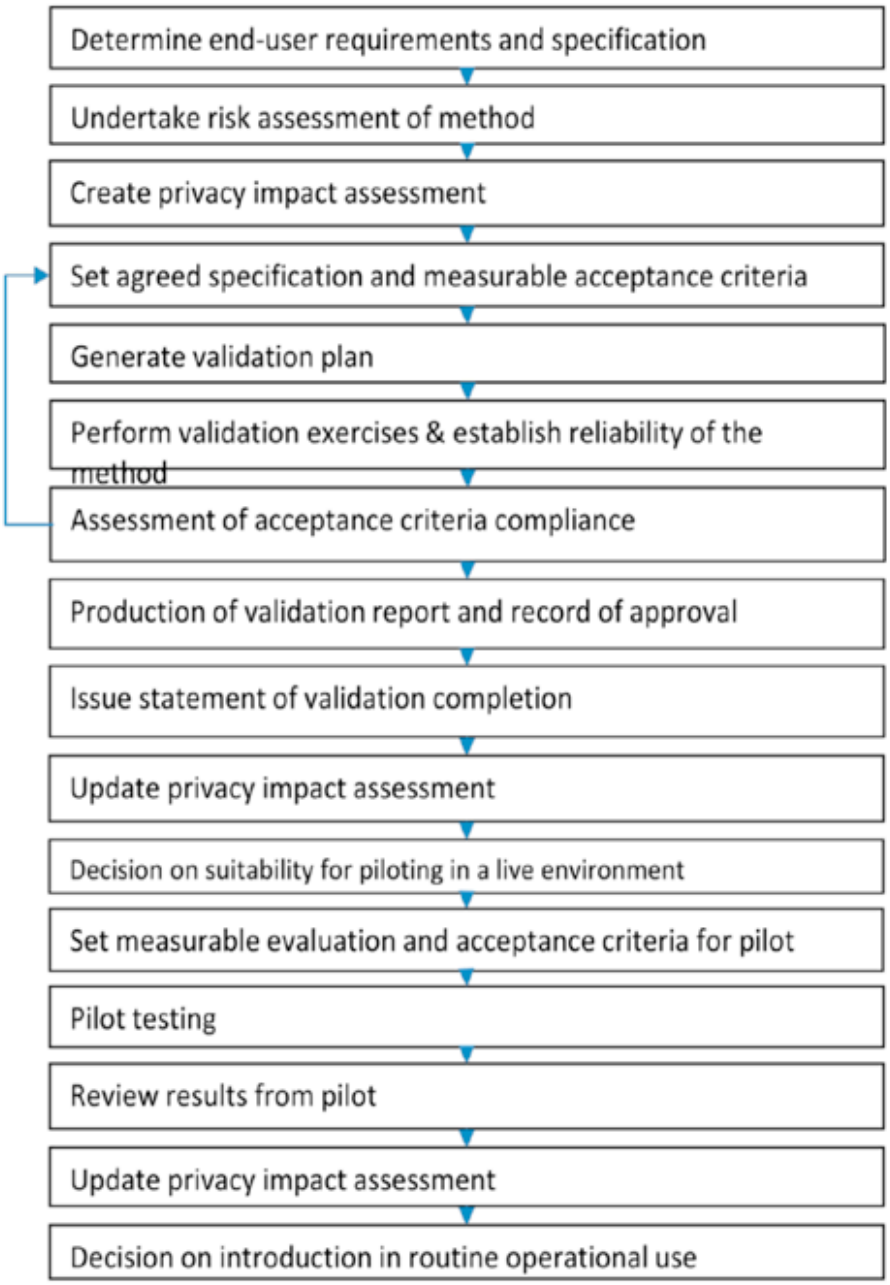
[47] Office of the Biometrics Commissioner (2018) 2017 Annual Report, London: HMSO para 308, pp 88- 89.

[48] Government Office for Science (2015) *Annual Report of the Government Chief Scientific Adviser 2015 Forensic Science and Beyond: Authenticity, Provenance and Assurance Evidence and Case Studies*, London: Government Office for Science, p38. Also often cited is additional guidance on test methodology has been set out by the Forensic Science Regulator, Forensic Science Regulator (2017) *Codes of Practice and Conduct for forensic science providers and practitioners in the Criminal Justice System*, Birmingham: The Forensic Science Regulator, (https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/651966/100_-_2017_10_09_-_The_Codes_of_Practice_and_Conduct_-_Issue_4_final_web_web_pdf__2_.pdf). However, the transferability of such guidance is brought into question by the argument that LFR cannot be regarded as a form of forensic science.

[49] The *Metropolitan Police Service Live Facial Recognition Trial Evaluation Methodology* also makes reference to a range of biometric evaluation standards. These include: ISO/IEC 19795-1:2006 Information technology – Biometrics performance testing and reporting – Part 1: Principles and Framework; ISO/IEC 19795-2:2007 Information technology - Biometric performance testing and reporting, Part 2: Testing methodologies for technology and scenario evaluation; ISO/IEC 19795-6: 2012 Information technology – Biometrics performance testing and reporting – Part 6: Testing methodologies for operational evaluation; ISO/IEC 30137-1: Information technology – Use of biometrics in video surveillance systems – Part 1: System design and specification; ISO/IEC 30137-2: Information technology – Use of biometrics in video surveillance systems – Part 2: Performance testing and reporting.

[50] Surveillance Camera Commissioner (2019) *The Police Use of Automated Facial Recognition Technology with Surveillance Camera Systems*, p 13. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/786392/AFR_police_guidance_of_PoFA_V1_March_2019.pdf.

Fig 1.1. Surveillance Camera Commissioner Defined Process for Piloting Automatic Facial Recognition



While the Surveillance Camera Commissioner's Office have been at the forefront of public debates around the governance of LFR such developments expose areas where clear national policy is needed. Multiple attempts have been made to insert elements of governance and oversight into the use of LFR technology. These include the establishment of a Home Office Biometrics Modalities board and interventions such as the Surveillance Camera Commissioner's guidance on 'The Police Use of Automated Facial Recognition Technology with Surveillance Camera Systems'. Debates exist over the comprehensiveness and reach of such governance

frameworks, and a clear gap exists with regards to the governance of the methodology and the practice of publicly trialling advanced surveillance technologies. Indeed, the Surveillance Camera Commissioner for England and underlined gaps in the governance framework and limitations of regulatory authority when interviewed for this report:

> […] my code […] is the only code of practice that oversees facial recognition and advancing technology, but [it] has not got any powers of sanction. Then you've got the biometric commissioner, who has no codified powers in relation to its use and actually his advice comes from the wealth of knowledge he's got about biometric use, but he doesn't yet have any statutory role in that… [not] everything's data protection…[51]

Not only does this raise challenges for accountability, ethics and the legal status of such trials, it places a notable burden on police teams who have a responsibility for upholding public safety. The absence of national leadership at government level and clear lines of responsibility regarding whether trials should be conducted, and if so how, leaves police evaluation teams with the enormous task of not only undertaking scientific evaluation, but also compensating for a lack of national leadership by recreating and reinterpreting policy anew.

The recent emergence of regional police-established independent ethics panels, normally staffed on a voluntary basis by independent experts, demonstrates the law enforcement community's desire to gain guidance and resolve these issues. These developments are, however, insufficient of themselves. The growth of advanced biometric surveillance and the pace of technological innovation mean that this issue is likely to arise frequently and recur with increasing rapidity. These issues are also generating significant levels of public debate and concern. Defined national leadership at government level over the legality, conduct, form and technical requirements for trialling such technologies is therefore vital to close gaps between increasing surveillance capability and effective oversight. Such leadership should establish clear and unambiguous lines of responsibility, be suitably independent and have the capacity to accommodate new and emerging forms of technology.

1.3.The scope of this report

The issues raised in the preceding section presented a problem when determining the scope of this report. A decision had to be made as to whether the focus should be narrow, focusing exclusively on the test deployments themselves, or whether it should be broader, incorporating analysis of potential future uses. The analysis contained in this report is primarily based on the empirical details of the six

[51] Interview with Tony Porter, Surveillance Camera Commissioner.

observed test deployments observed. However, the decision was made to accommodate a somewhat broader approach with respect to Section 2 and, to a lesser extent, Section 3. Two principal factors were relevant. First, the stated aim of the trials was broad. For instance, objectives as stated by the MPS were 'to assess the situations under which LFR technology can be used as a viable and effective policing tactic',[52] and to evaluate LFR technology 'as an overt means of tracing wanted persons and enhancing safety at public events.'[53] These are broad objectives and no indication was provided that post-trial deployments would be restricted to the narrow circumstances of use adopted during the trials.[54] Indeed, given the significant resource implications, it is unlikely that future deployments would seek to replicate trial conditions. Second, in conversations with members of the MPS team responsible for the trials, the possibilities regarding broad future uses of LFR technology were discussed. For instance, the possibility that LFR software could be integrated into the public transport surveillance network was raised. As such, while this report remains focused on the trials conducted between 2016 and 2019, it is not blind to other potential future uses.

1.4.The Structure of this Report

This report first outlines key human rights law considerations relevant to the deployment of LFR technology (Section 2) before examining the process surrounding the test deployments themselves. This analysis is divided between the pre-test planning phase (Section 3) and the deployment phase (Section 4).

Section 2 discusses the human rights law considerations relevant to the deployment of LFR in general terms. It is not applied specifically to the activities of the MPS. Instead, this section is intended to provide a foundation for the analysis conducted in Sections 3 and 4.

Section 3 examines how the MPS approached the pre-test deployment phase. This section analyses: the MPS' identification of research objectives and the development of a methodology appropriate to these objectives; the identification of an appropriate legal basis to underpin the test deployments; efforts undertaken to meet the 'necessity' test; and how transparency was handled, including the public availability of information on the test deployments, and issues relating to community engagement.

[52] 'Live Facial Recognition, (LFR) MPS Legal Mandate', 23 July 2018, p.3.
[53] 'Data Protection Impact Assessment for the use of Live Facial recognition within the MPS', 12 February 2019, p. 2.
[54] This was noted by Silkie Carlo, Director of Big Brother Watch: '[The trials are] not an actual representation of how this could ever realistically be deployed operationally. You can never just stick a van and have 20 officers around, so, yes, it's inevitably going to go down the route of body worn, mobile, etc.'. Interview with Silkie Carlo, Director, Big Brother Watch.

Section 4 focuses on the test deployments themselves. This section examines: the process of constructing the watchlist, including any variations across the test deployments; how intelligence was matched to the operational deployments; the concept of consent, and how consent-based policing was approached; the process surrounding real-time LFR matches, with a particular focus on the adjudication process, the role of discretion, and variations in practice; the impact of different communications technologies on the test deployments; spatial characteristics relevant to the placement of cameras and officers; the various operational settings; and how interactions engaging members of the public were resolved.

2. Human Rights Law Considerations

Given the rapidly evolving nature of modern technology, and the significant – often previously unimagined – capabilities presented, the argument is frequently made that law or oversight cannot keep pace.[55] The authors disagree with this claim. Human rights law provides an organising framework for the design, development, and deployment of advanced technologies such as LFR.[56] As such, it can play a key role in ensuring that police forces can indeed 'strike the right balance' referred to in *S and Marper*.[57] For instance, human rights law provides a means of identifying the potential 'harm' associated with the deployment of particular technologies, of evaluating different competing interests (such as public order considerations and the rights of affected individuals), and determining whether particular activities are permissible or not. It also provides concrete guidance regarding the specific obligations placed on the State and State authorities (such as the police constabularies), and establishes criteria applicable to safeguards and oversight.

Taking this position as a starting point, the purpose of this section is to set out the human rights law considerations relevant to law enforcement uses of LFR, in general terms, in order to inform the analysis of MPS activities as presented in Sections 3 and 4. It is based on the understanding that human rights law compliance is a prerequisite for any policing activity. All of the human rights considerations discussed here are codified in the European Convention on Human Rights, and given further effect to by the Human Rights Act 1998.[58] These provisions are binding on all UK police constabularies.[59]

This section will focus on two key issues. First, the range of rights brought into play by police uses of LFR are discussed. The overall rights impact extends beyond the right to privacy and it is important that broader rights considerations are incorporated into any impact assessment so that an effective necessity and proportionality analysis can be conducted.[60] Second, the human rights law test established to regulate interferences with human rights protections will be examined. As developed in the case law of the European Court of Human Rights, this is a three-part test requiring that any rights interference be in accordance with

[55] See, for instance, Lee Rainie & Janna Anderson, 'Code-Dependent: Pros and Cons of the Algorithm Age', Pew Research Center, 8 January 2017.
[56] See further, Lorna McGregor, Daragh Murray & Vivian Ng, 'International Human Rights Law as a Framework for Algorithmic Accountability' (2019) 68 International and Comparative Law Quarterly.
[57] *S. and Marper v. the United Kingdom*, Judgment, ECtHR, App. Nos. 30562/04 & 30566/04, 4 December 2008, para. 112.
[58] UK Human Rights Act 1998. Available at: https://www.legislation.gov.uk/ukpga/1998/42/contents. See Section 1 of this Act for the meaning of 'Convention rights'.
[59] See, Section 6(1), Human Rights Act 1998, concerning public authorities.
[60] Regarding the range of rights brought into play, see for example, Surveillance Camera Commissioner, 'Police Use of Automated Facial Recognition Technology with Surveillance Camera Systems: Section 33 Protection of Freedoms Act 2012', March 2019, p. 3.

the law (necessitating an appropriate legal basis), pursue a legitimate aim, and be necessary in a democratic society.[61]

The leading role played by UK police forces in the development of LFR technology demands that particular attention be paid to human rights compliance. The decision of the European Court of Human Rights in *S and Marper v. the U.K.* – which addresses the retention of DNA, fingerprints, and cellular samples – is considered relevant in this regard:

> The protection afforded by [the right to private life] would be unacceptably weakened if the use of modern scientific techniques in the criminal justice system were allowed at any cost and without carefully balancing the potential benefits of the extensive use of such techniques against important private-life interests. […] The Court considers that any State claiming a pioneer role in the development of new technologies bears special responsibility for striking the right balance in this regard.[62]

2.1. Identification of Rights Potentially Affected by the Deployment of LFR Technology

The range of human rights potentially affected by police deployments of LFR technology is dependent upon a number of factors including, but not limited to, the formulation of the watchlist, the nature of specific deployments, the interconnectivity of different camera and information/intelligence systems, and the use of automated analysis software. The right to privacy is, of course, a key concern. However, it is important to note that the right to privacy is not the only right that is brought into play, and that any impact assessment should consider the full range of rights implications.

Impact or risk assessments are not an explicit requirement of human rights law. However, they are a key means by which (a) the obligation to respect human rights,[63] and (b) the requirement to ensure that any rights interference is necessary in a democratic society,[64] can be fulfilled.[65] In this regard the Surveillance Camera Commissioner has noted that

[61] *Big Brother Watch and Others v. the United Kingdom*, Judgment, ECtHR, App. Nos. 58170/13, 62322/14, 24960/15, 13 September 2018, para. 304; *Times Newspapers Ltd (Nos. 1 and 2) v. the United Kingdom*, Judgment, ECtHR, App. Nos. 3002/03, 23676/03, 10 March 2009, para. 37.

[62] *S. and Marper v. the United Kingdom*, Judgment, ECtHR, App. Nos. 30562/04 & 30566/04, 4 December 2008, para. 112.

[63] Article 1, European Convention on Human Rights. The obligation to respect requires, *inter alia*, that States (or public authorities) not take any measures that directly violate human rights. In order to ensure respect for rights, some form of impact assessment is therefore required.

[64] For further discussion in this regard see Section 2.2.3.

> The use of [LFR] has the potential to impact upon ECHR rights and thereby influence the sense of trust and confidence within communities. It should be a fundamental consideration of any relevant authority intending to deploy [LFR] that a detailed risk assessment process is conducted and documented as to the operational risks, community impact risk, privacy and other human rights risk and other risks associated with its use prior to any deployment of the capability is made. Such risks should be considered as part of the decision making processes associated with the necessity and proportionality of its use.[66]

The creation of a Data Protection Impact Assessment does constitute a legal requirement in the UK. This duty was outlined by the Information Commissioner's Office submission to this report as follows:

> Part 3 of the Data Protection Act 2018 (DPA18) applies to competent authorities when processing personal data for law enforcement purposes. Competent authorities are listed under Schedule 7 of the DPA, and also extends to bodies with statutory functions for criminal law enforcement functions, which includes police forces. The processing of biometric data to uniquely identify an individual falls into the category of sensitive processing under DPA18 (s35 (8)). This applies to the processing of data using automated facial recognition.
>
> In order to be compliant under DPA18, police forces need to be able to demonstrate that they are using AFR for law enforcement purposes. As the processing involves sensitive data, particular safeguards apply: the processing must be strictly necessary; a condition under Schedule 8 is applicable, and an appropriate policy document should be in place to describe how sensitive personal data is processed.

This subsection will discuss some of the rights that the deployment of LFR technology may engage.[67] As noted above, the use of LFR constitutes biometric processing,[68] thereby brining into play data protection considerations.[69] These data protection considerations – although not discussed further herein – will necessarily

[65] For more detailed discussion see, UN Human Rights Council, 'Report of the Office of the UN High Commissioner for Human Rights on 'The Role of Prevention in the Promotion and Protection of Human Rights'' (16 July 2015) UN Doc. A/HRC/30/20, paras. 7-9.
[66] Surveillance Camera Commissioner, 'Police Use of Automated Facial Recognition Technology with Surveillance Camera Systems: Section 33 Protection of Freedoms Act 2012', March 2019, p. 9.
[67] As noted, the specific rights affected in any LFR deployment is dependent on a number of different factors and the discussion presented herein is for background purposes. Other rights may be brought into play, dependent on the circumstances of use.
[68] See Section **Error! Reference source not found.**. This was also emphasised by the Information Commissioner's Office.
[69] Of principal relevance are the Data Protection Act 2018, and the Law Enforcement Directive.

overlap with privacy considerations.[70] Indeed, this interconnection between data protection law and the right to privacy is underlined by the classification of biometric data as a particularly sensitive form of personal information.[71] Equally, it is highlighted that different rights considerations will be brought into play at different stages of LFR activity.[72] For instance, the initial biometric processing of information will give rise to specific considerations, the subsequent retention of information – and access to that information – will give rise to specific considerations, as will any subsequent analysis – automated or otherwise – of the retained information.

Before proceeding further, it should be clarified that the term 'interference' is used when a particular right is brought into play, or 'engaged'. The existence of an interference should then prompt a determination as to whether this interference is legitimate or not, and thus whether it results in a violation of the right in question, or not. For clarity, it is emphasised that the existence of an interference with a right does not, of itself, equate to a violation of that right.

2.1.1. The Right to Privacy

The right to privacy is codified in Article 8 of the European Convention on Human Rights. It establishes that:

> 8(1). Everyone has the right to respect for his private and family life, his home and his correspondence.

This is a 'qualified' right and interferences with the right to privacy are permitted under certain conditions:

> 8(2). There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

The European Court of Human Rights has established that '[p]rivate life is a broad term not susceptible to exhaustive definition.'[73] The Court has clarified, however, that the right to private life incorporates elements related to an individual's personal sphere – such as their sexual orientation or health information – as well as 'a right to identity and personal development, and the right to establish relationships with

[70] For instance, a number of the cases referred to below in the context of the right to privacy – such as those relating to fingerprints or DNA samples also give rise to data protection considerations. See further Section 2.1.1.
[71] Section 35, Data Protection Act 2018.
[72] Necessarily many of the rights considerations at different stages of LFR usage may overlap. The issue is that distinct analysis vis-à-vis the rights implications may be required at each stage.
[73] *Peck v. the United Kingdom*, Judgment, ECtHR, App. No. 44647/98, 28 January 2003, para. 57.

other human beings and the outside world'.[74] The right to private life may therefore include activity taking place in a public context.[75]

The question therefore arises as to whether LFR technology deployed overtly in a public place may be said to constitute an interference with the right to privacy.[76] Although this issue has not been addressed directly by the courts, existing case law of the European Court of Human Rights does offer concrete guidance.

As a starting point, it is noted that the mere observation or monitoring of an individual in a public place, without further analysis, does not give rise to an interference with the right to private life.[77] For instance, the European Court of Human Rights has held that,

> '[a] person who walks down the street will, inevitably, be visible to any member of the public who is also present. Monitoring by technological means of the same public scene (for example, a security guard viewing through closed-circuit television) is of a similar character.'[78]

However, private life considerations do come into play if, instead of merely being monitored, elements of a public scene are recorded or subject to processing.[79] For instance, the European Court has held that 'private life considerations may arise concerning the recording of [photographic] data and the systematic or personal nature of the recording.'[80] Equally, while an individual's questioning by police officers may not bring into play the right to private life, the recording of their voice for further analysis is regarded as the processing of personal data, thereby constituting an interference with the right to private life.[81] Photographs of an individual have been held to constitute personal data,[82] and the European Court has clearly stated that:

---

[74] *Peck v. the United Kingdom*, Judgment, ECtHR, App. No. 44647/98, 28 January 2003, para. 57.
[75] *Antovic and Mirkovic v. Montenegro*, Judgment, ECtHR, App. No. 70838/13, 28 November 2017, para. 43; *Peck v. the United Kingdom*, Judgment, ECtHR, App. No. 44647/98, 28 January 2003, para. 57.
[76] Concerns exist regarding the classification of LFR as an 'overt' form of surveillance. See for instance, Surveillance Camera Commissioner (2019) *The Police Use of Automated Facial Recognition Technology with Surveillance Camera Systems*, para 10(2). Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/786392/AFR_police_guidance_of_PoFA_V1_March_2019.pdf.
[77] *Perry v. the United Kingdom*, Judgment, ECtHR, App. No. 63737/00, 17 July 2003, para. 38.
[78] *P.G. and J.H. v. the United Kingdom*, Judgment, ECtHR, App. No. 44787/98, 25 September 2001, para. 57. See also, *Peck v. the United Kingdom*, Judgment, ECtHR, App. No. 44647/98, 28 January 2003, para. 59.
[79] *P.G. and J.H. v. the United Kingdom*, Judgment, ECtHR, App. No. 44787/98, 25 September 2001, para. 57.
[80] *Lopez Ribalda and Others v. Spain*, Judgment, ECtHR, App. Nos. 1874/13, 8567/13, 9 January 2018, para. 56 (referral to GC pending).
[81] See the Court's discussion in this regard *in Peck v. the United Kingdom*, Judgment, ECtHR, App. No. 44647/98, 28 January 2003, para. 59. See also, *AB and Hampshire Constabulary*, Judgment, Investigatory Powers Tribunal, Case No. IPT/17/191/CH, 5 February 2019.
[82] *Szabo and Vissy v. Hungary*, Judgment, ECtHR, App. No. 37138/14, 12 January 2016, para. 96.

> A person's image constitutes one of the chief attributes of his or her personality, as it reveals the person's unique characteristics and distinguishes the person from his or her peers. The right to the protection of one's image is thus one of the essential components of personal development and presupposes the right to control the use of that image.'[83]

As LFR technology involves the biometric processing of a person's image, an analogy may also be drawn to case law addressing fingerprints and DNA samples, which have been held to give rise to considerations regarding the right to private life.[84]

A decision of the European Commission on Human Rights is relevant to the deployment of LFR technology:

> In *Friedl*, the Commission considered that the retention of anonymous photographs that have been taken at a public demonstration did not interfere with the right to respect for private life. In so deciding, it attached special weight to the fact that the photographs concerned had not been entered into a data-processing system and that the authorities had taken no steps to identify the persons photographed by means of data processing.[85]

It is clear that the use of LFR technology involves the biometric processing of images taken in a public place, for the purpose of determining an individual's identity, and the potential retention of those images. As such, and in light of the case law discussed above relating to the recording and processing of data, including personal data, it is submitted that both the initial biometric processing of images (i.e. their analysis by means of LFR technology), and any subsequent retention of video footage,[86] constitute separate interferences with the right to private life.

2.1.2. The Rights to Freedom of Expression and the Right to Freedom of Assembly and Association

The deployment of LFR technology may generate a chilling effect whereby individuals refrain from lawfully exercising their democratic rights due to a fear of the consequences that may follow.[87] For instance, they may be reluctant to meet with

[83] *Reklos and Davourlis v. Greece*, Judgment, ECtHR, App. No. 1234/05, 15 April 2009, para. 40.
[84] See, *S. and Marper v. the United Kingdom*, Judgment, ECtHR, App. Nos. 30562/04 & 30566/04, 4 December 2008, para. 112.
[85] *S. and Marper v. the United Kingdom*, Judgment, ECtHR, App. Nos. 30562/04 & 30566/04, 4 December 2008, para. 82, referring to *Friedl v. Austria*.
[86] Should retained footage be subject to further analysis, additional rights considerations may arise.
[87] The precise contours of any chilling effect are contested, but research points to its existence. See, J. Penney, 'Chilling effects: Online surveillance and Wikipedia use', 31 *Berkeley Technology Law Journal* (2016) 117; E. Stoycheff 'Under Surveillance:

particular individuals or organizations, to attend particular meetings, or to take part in particular protests, at least in part due to the fear of 'guilt by association'.

The ability to engage in this form of activity is protected by the right to freedom of expression,[88] and the right to freedom of assembly and association,[89] both individually and when these rights act in conjunction with each other. The right to privacy is also relevant, as an individual's ability to act anonymously is a significant counterbalance to any chilling effect. For illustrative purposes, this section will focus on the right to freedom of expression.

The right to freedom of expression is codified in Article 10 of the European Convention on Human Rights. It establishes that:

> 10(1). Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. This Article shall not prevent States from requiring the licensing of broadcasting, television or cinema enterprises.
> 2. The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary.

The European Court of Human Rights has held that '[f]reedom of expression constitutes one of the essential foundations of a democratic society and one of the basic conditions for its progress and for each individual's self-fulfilment'.[90] The importance of the right is clearly stated:

> there can be no democracy without pluralism. Democracy thrives on freedom of expression. It is of the essence of democracy to allow diverse political programmes to be proposed and debated, even those that call

Examining Facebook's Spiral of silence Effects in the Wake of NSA Internet Monitoring', 93 *Journalism and Mass Communication Quarterly* (2016) 296, and for a general discussion Daragh Murray & Pete Fussey, 'Bulk Surveillance in the Digital Age: Rethinking the Human Rights Law Approach to Bulk Monitoring of Communications Data' (2019) 52 Israel Law Review 1. For discussion regarding the chilling effect as applicable to journalists, see *Centro Europa 7 S.R.L. and Di Stefano v. Italy*, Judgment, European Court of Human Rights, App. No. 38433/09, 7 June 2012, para. 129.

[88] Article 10, European Convention on Human Rights.

[89] Article 11, European Convention on Human Rights.

[90] *Case of Mouvement Raelien Suisse v. Switzerland*, Judgment, ECtHR, App. No. 16354/06, 13 July 2012, para. 48.

> into question the way a State is currently organised, provided that they do not harm democracy itself.[91]

Accordingly, the right to freedom of expression protects both the right to receive and to impart information,[92] and 'is applicable not only to "information" or "ideas" that are favourably received or regarded as inoffensive or as a matter of indifference, but also to those that offend, shock or disturb the State or any sector of the population.'[93]

Existing academic research from other jurisdictions indicates that police use of overt surveillance technology may impair political protest movements, thereby bringing the right to freedom of expression – and the right to freedom of association and assembly – into play. This research suggests that:

> police surveillance was perceived as being i) physically and psychologically intrusive, ii) restricting social and political interaction and iii) reducing autonomy. It was also reported to be disruptive of collective political freedoms by reducing internal and external perceptions of legitimacy and safety, creating divisions and deterring participation.[94]

As noted by Purhouse and Campbell in an academic legal analysis of LFR:

> overt surveillance can damage legitimate political mobilisations in public space by undermining the perceived legitimacy of protest groups and limiting their access to resources. These findings, which are supported by empirical research from the US, suggest that the presence of visible surveillance at meetings and other political gatherings will reduce perceptions of legitimacy, and harm the efforts of such groups to be taken seriously and attract support from their target audiences. The reputational hit that political groups may take when they are subject to surveillance can also have a knock-on effect on resources and networks.[95]

This chilling effect has clear implications vis-à-vis the effective functioning of a participatory democracy, and therefore directly brings into play the right to freedom of expression. These rights will be of enhanced relevance if, for example, LFR

[91] *Centro Europa 7 S.R.L. and Di Stefano v. Italy*, Judgment, ECtHR, App. No. 38433/09, 7 June 2012, para. 129.
[92] *Ahmet Yildirim v. Turkey*, Judgment, ECtHR, App. No. 3111/10, 18 December 2012, para. 50.
[93] *Handyside v. the United Kingdom*, Judgment, ECtHR, App. No. 5493/72, 7 December 1976, para. 49.
[94] Valerie Aston, 'State surveillance of protest and the rights to privacy and freedom of assembly: a comparison of judicial and protester perspectives' (2017) 8 European Journal of Law and Technology 1, 2.
[95] Joe Purshouse & Liz Campbell, 'Privacy, crime control and police use of automated facial recognition technology' (2019) Criminal Law Review 3, 196.

technology is integrated into body worn cameras or open street surveillance camera networks, or subject to further analysis.

2.1.3. The Prohibition of Discrimination

The prohibition of discrimination is codified in Article 14 of the European Convention on Human Rights. It establishes that:

> The enjoyment of the rights and freedoms set forth in this Convention shall be secured without discrimination on any ground such as sex, race, colour, language, religion, political or other opinion, national or social origin, association with a national minority, property, birth or other status.

Article 14 applies in relation to the rights codified in the European Convention on Human Rights, and guarantees that those rights should be enjoyed without discrimination.[96] For example, in the context of LFR deployments Article 14 might apply in conjunction with Article 8, if particular individuals are more vulnerable to privacy infringements due to algorithmic bias relating to sex, race, or ethnicity. In the UK, the Equality Act 2010 also prohibits discrimination, in and of itself. That is, discrimination does not have to occur in relation to a particular Convention right in order for it to be unlawful. Instead, the criteria for discrimination rests on differential treatment on the basis of a protected characteristic.[97]

The prohibition of discrimination relates to both direct and indirect discrimination. Direct discrimination relates to intentional discrimination on the basis of one of the prohibited grounds. As such, demonstrating direct discrimination requires proving that others are treated differently on the basis of a protected characteristic, when they are in a comparable situation.[98] Indirect discrimination occurs when an act appears neutral on its face, but has the effect of discriminating. The European Court of Human Rights described indirect discrimination as follows:

> … a difference in treatment may take the form of disproportionately prejudicial effects of a general policy or measure which, though couched in neutral terms, discriminates against a group […] such a situation may amount to 'indirect discrimination', which does not necessarily require a discriminatory intent.[99]

[96] It is therefore distinct from broad anti-discrimination provision as established, for example, in the Equality Act 2010.
[97] See, for instance, Chapter 2, Equality Act 2010.
[98] See, *Lithgow v the United Kingdom*, Judgment, ECtHR, App. Nos. *9006/80, 9262/81, 9263/81, 9265/81, 9266/81, 9313/81, 9405/81*, 8 July 1986, para. 177.
[99] *D.H. and Others v. the Czech Republic*, Judgment ECtHR, App. No. 57325/00, 13 November 2007, para. 184.

Applied to the use of LFR technology, the prohibition of discrimination requires that all those subject to the technology be treated in the same manner, and that there be no difference in treatment – either directly or indirectly – on the basis of one or more of the protected characteristics.[100] This is a concern in relation to the use of LFR technology in at least two ways, relating to technical performance and police deployments. First, concerns have been raised regarding bias built into LFR technology. This means that the technology may behave differently depending upon an individual's sex, race, or colour, thereby giving rise to indirect discrimination. Second, LFR technology may be deployed in a manner that gives rise to concerns regarding discrimination. This is more analogous to traditional concerns associated with potentially discriminatory policing practices,[101] and – applied to LFR - may depend on factors such as input data and watchlist composition, or the nature of the deployment.

The prohibition of discrimination requires that police forces take measures to ensure that neither the LFR technology nor its means of deployment violate the prohibition of discrimination.[102]

2.2.Evaluating the Legitimacy of an Interference with Human Rights

As discussed in the previous section, the use of LFR technology can bring into play a number of human rights, thereby constituting an 'interference' with those rights. However, as noted above an interference does not necessarily amount to a violation, and in order to evaluate the legitimacy of any interference a three-part test is applied. An interference with the right to privacy, the right to freedom of expression, or the right to freedom of association and assembly will be lawful if it is: in accordance with the law, pursues a legitimate aim, and is necessary in a democratic society in order to achieve that aim.[103] These three elements will be examined in turn.

2.2.1. Is an Interference 'In Accordance with the Law'?

The purpose of this requirement is to protect against the arbitrary exercise of State power. As such, any measure interfering with human rights protections must have a legal basis, and that legal basis must be of sufficient quality to protect against

[100] See Section 1.2.2 for further discussion regarding bias and discrimination in relation to the use of LFR technology.
[101] See for instance, concerns raised by Liberty regarding potential discrimination associated with the use of stop and search, Liberty, 'Stop and Search: the Facts', available at: https://www.libertyhumanrights.org.uk/tags/stop-and-search. See also, concerns regarding Operation Champion which involved the use of surveillance cameras in predominantly Muslim areas of Birmingham, 'Birmingham Project Champion 'spy' cameras being removed', *BBC News*, 9 May 2011, available at: https://www.bbc.co.uk/news/uk-england-birmingham-13331161.
[102] See further, Section 149, Equality Act 2010.
[103] *Big Brother Watch and Others v. the United Kingdom*, Judgment, ECtHR, App. Nos. 58170/13, 62322/14, 24960/15, 13 September 2018, para. 304.

arbitrary rights interferences.[104] This requires that a number of different elements be satisfied:

> …the expression "in accordance with the law" not only requires the impugned measure to have some basis in domestic law, but also refers to the quality of the law in question, requiring that it should be accessible to the person concerned and foreseeable as to its effects. For domestic law to meet these requirements, it must afford adequate legal protection against arbitrariness and accordingly indicate with sufficient clarity the scope of discretion conferred on the competent authorities and the manner of its exercise[105]

It is evident, therefore, that the legal basis must be of sufficient clarity to delimit the circumstances in which a particular measure may be deployed, such that those circumstances are foreseeable, thereby protecting against arbitrary rights interference. As stated by the European Court of Human Rights, on the basis of well-established case law, '[t]he law must thus be adequately accessible and foreseeable, that is, formulated with sufficient precision to enable the individual – if need be with appropriate advice – to regulate his conduct.'[106]

In *Catt v. the United Kingdom* the European Court further stressed that, although elements of its case law may focus on covert measures of surveillance, in circumstances where 'the powers vested in the state are obscure, creating a risk of arbitrariness especially where the technology is continually becoming more sophisticated […] it should be guided by this approach [developed regarding covert measures] especially where it has already highlighted concerns relating to the ambiguity of the state's powers.'[107] The approach referred to focused on the development of appropriate legal safeguards,[108] and detailed rules regarding appropriate circumstances of use.[109] Of relevance in this regard is the decision in *Big Brother Watch and Others v the United Kingdom* which held that: '[t]he domestic law must be sufficiently clear to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to any such measures.'[110]

Catt related to the retention of information on an individual following overt surveillance of their participation in protests, and their association with a group

[104] *Shimovolos v. Russia*, Judgment, ECtHR, App. No. 30194/09, 21 June 2011, para. 67.
[105] *Catt v. the United Kingdom*, Judgment, ECtHR, App. No. 43514/15, 24 January 2019, para. 94.
[106] *S. and Marper v. the United Kingdom*, Judgment, ECtHR, App. Nos. 30562/04 & 30566/04, 4 December 2008, para. 95.
[107] *Catt v. the United Kingdom*, Judgment, ECtHR, App. No. 43514/15, 24 January 2019, para. 114.
[108] *Szabo and Vissy v. Hungary*, Judgment ECtHR, App. No. 37138/14, 12 January 2016, para. 68.
[109] *Zakharov v. Russia*, Judgment, ECtHR, App. No. 47143/06, 4 December 2015, para. 229.
[110] *Big Brother Watch and Others v. the United Kingdom*, Judgment, ECtHR, App. Nos. 58170/13, 62322/14, 24960/15, 13 September 2018, para. 306.

which had engaged in violent demonstrations. However, the reasoning is equally applicable to the use of LFR technology. The rapidly changing capacity of this technology, and the ambiguity surrounding its legal basis and circumstances of use are pertinent factors in this regard. As such, the legal basis regulating the use of LFR technology should be clear, foreseeable regarding circumstances of deployment, and accompanied by appropriate safeguards and rules on circumstances of use.[111] The publication of safeguards and rules on use online may contribute towards the foreseeability of any measures. For instance, in *Kennedy v. the United Kingdom* the European Court of Human Rights held that the online publication of a code of practice relating to the Regulation of Investigatory Powers Act 2000 (RIPA) could be taken into account when evaluating the foreseeability of RIPA itself.[112] A similar finding was made in *Big Brother Watch v. the United Kingdom*.[113] The existence of publicly available guidance is likely to be particularly important in the absence of an explicit legal basis.

S and Marper v. the United Kingdom highlighted the need for appropriate safeguards, with specific reference to personal data:

> The protection of personal data is of fundamental importance to a person's enjoyment of his or her right to respect for private and family life, as guaranteed by Article 8 of the Convention. The domestic law must afford appropriate safeguards to prevent any such use of personal data as may be inconsistent with the guarantees of Article 8 […] The need for such safeguards is all the greater when the protection of personal data undergoing automatic processing is concerned, not least when such data are used for police purposes.[114]

2.2.2. Does an Interference 'Pursue a Legitimate Aim'?

Any rights interference must pursue a legitimate aim, as detailed in the limitation clause of the relevant right. With respect to the right to privacy, the legitimate aims are:

> the interests of national security, public safety or the economic well-being of the country, the prevention of disorder or crime, the protection

[111] For further discussion regarding the protection against arbitrary rights interference, the scope of discretion, and the existence of appropriate safeguards regulating particular powers see, *Beghal v. the United Kingdom*, Judgment, ECtHR, App. No. 4755/16, 28 February 2019, paras. 87-110.
[112] *Kennedy v. the United Kingdom*, Judgment, ECtHR, App. No. 26839/05, 18 May 2010, para. 157.
[113] *Big Brother Watch and Others v. the United Kingdom*, Judgment, ECtHR, App. Nos. 58170/13, 62322/14, 24960/15, 13 September 2018, para. 325.
[114] *S. and Marper v. the United Kingdom*, Judgment, ECtHR, App. Nos. 30562/04 & 30566/04, 4 December 2008, para. 103.

> of health or morals, or the protection of the rights and freedoms of others[115]

With respect to the right to freedom of expression, the legitimate aims are:

> the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary[116]

It is generally accepted that policing activity pursues the legitimate aim of preventing disorder or crime, and protecting the rights of others.[117] As such, no significant concerns are raised regarding the legitimate aim pursued by police deployment of LFR technology.

2.2.3. Is the Interference 'Necessary in a Democratic Society'?

The final component of the three-part test examines whether the interference is necessary in a democratic society. This is essential in order to ensure the overall rights compliance of any measure, and in this context it is intended to ensure that measures useful to the protection of public order and the prevention of crime do not inappropriately undermine other rights, including those necessary to the effective functioning of a democratic society, such as the right to private life, the right to freedom of expression, and/or the right to freedom of assembly and association. The necessity test is intended to address the 'competing interests'[118] arising in this regard. In order to determine these competing interests, and to effectively determine the necessity of a measure, it is essential that the full range of rights brought into play be identified.[119]

The test itself involves a number of different elements. An interference will be considered necessary in a democratic society 'if it answers to a "pressing social need", if it is proportionate to the legitimate aim pursued and if the reasons adduced by the national authorities to justify it are relevant and sufficient.'[120] It is important to note that the necessary in a democratic society test does not straightforwardly equate to a proportionality test (as conventionally understood).[121] Rather, the measure must

---

[115] Article 8(2), European Convention on Human Rights.
[116] Article 10(2), European Convention on Human Rights.
[117] See, for instance, *Catt v. the United Kingdom*, Judgment, ECtHR, App. No. 43514/15, 24 January 2019, para. 108.
[118] *S. and Marper v. the United Kingdom*, Judgment, ECtHR, App. Nos. 30562/04 & 30566/04, 4 December 2008, para. 112.
[119] See above, Section 2.1.
[120] *Catt v. the United Kingdom*, Judgment, ECtHR, App. No. 43514/15, 24 January 2019, para. 109.
[121] A conventional understanding of proportionality may be based on the understanding that a measure is permissible if the benefit is proportionate to the interference with an individual's right(s).

first be deemed necessary in a democratic society, and then the specific means of implementation must satisfy the proportionality test.[122] This is an important distinction as it establishes a stricter overall test: the necessity in a democratic society of a measure is first determined, and then the measure must be examined to ensure that it does not go beyond that which is necessary (i.e. it is not disproportionate).[123]

This distinction may be demonstrated by reference to issues arising in relation to the retention of custody images or fingerprints.[124] It may be considered necessary in a democratic society to retain images of those convicted of an offence, but not of those who have been detained, questioned, or prosecuted, but not convicted. Key here is the risk of stigmatisation,[125] and the impact on rights such as the right to private life. The proportionality test will then focus on the modalities of retention, such as the length of retention, who may access an image/fingerprint, procedures for deletion, and so on. This example highlights that a measure may be necessary in a democratic society in relation to certain purposes but not for others. In the context of LFR a number of factors are therefore relevant when considering necessity. These include the nature of the deployments, the interconnectivity of different facial recognition systems, any analysis performed, and the formulation of watchlists.

Building on the decision in *Catt* that, in certain circumstances, the approach to covert surveillance should guide overt techniques, a further factor may be relevant to the necessity test.[126] The case law of the European Court of Human Rights and the Court of Justice of the European Union has clearly established that - due to the nature of the rights interference[127] - covert surveillance may not be justified in relation to all crimes or intelligence activities, and that a threshold must therefore be established. In this regard it has been held that large-scale covert surveillance may only be justified in relation to 'serious crime'.[128] As stated by the Court of Justice of the European Union in *Watson*:

---

[122] See, *Handyside v. the United Kingdom*, Judgment, ECtHR, App. No. 5493/72, 7 December 1976, para. 49. Confusion does exist as to the relationship between the necessary in a democratic society test and the proportionality test, with the two often treated as synonymous. This is only appropriate if the proportionality test conducted is broad, i.e. if it takes into account the requirements of a democratic society and the competing interests that arise in relation to the measure in question. A narrow reading of proportionality is inconsistent with the human rights law requirements.

[123] Although formulated somewhat differently in English case law, the test is effectively equivalent to that presented here. It focuses, *inter alia*, on whether the 'objective of the measure is sufficiently important to justify the limitation of a protected right' (i.e. is it necessary) and whether 'a less intrusive measure could have been used' and 'whether, balancing the severity of the measure's effects on the rights of the persons to whom it applies against the importance of the objective, to the extent that the measure will contribute to its achievement, the former outweighs the latter' (i.e. is it proportionate). See, *Bank Mellat v HM Treasury (No 2)* [2013] UKSC 39, [2014] AC 700, para. 74.

[124] See, in this regard *S. and Marper v. the United Kingdom*, Judgment, ECtHR, App. Nos. 30562/04 & 30566/04, 4 December 2008, and *RMC and FJ v. Commissioner of Police of the Metropolis* [2012] EWHC 1681 (Admin).

[125] The European Court of Human Rights discussed the risk of stigmatisation in the context of the presumption of innocence. See, *S. and Marper v. the United Kingdom*, Judgment, ECtHR, App. Nos. 30562/04 & 30566/04, 4 December 2008, para. 122.

[126] *Catt v. the United Kingdom,* Judgment, ECtHR, App. No. 43514/15, 24 January 2019, para. 114.

[127] *Tele2 Sverige AB v Post-och telestyrelsen* and *Secretary of State for the Home Deprtment v. Watson and others*, Judgment, Grand Chamber, Court of Justice of the European Union, Cases C-203/15, C-698/15, 21 December 2016, para. 102.

[128] In this regard the Court of Justice of the European Union has referred to threats to national security and activities that will affect the monetary stability of the state. See, *Rechbnungshof v. Osterreichischer Rundfunk and Others*, Judgment, Court of Justice

> since the objective pursued [...] must be proportionate to the seriousness of the interference in fundamental rights that access entails, it follows that, in the area of prevention, investigation, detection and prosecution of criminal offences, only the objective of fighting serious crime is capable of justifying such access to the retained data.[129]

This may indicate that, if LFR is deemed necessary in a democratic society in principle, its use may be restricted. Any such restrictions are likely to relate to the place of deployment[130] or the nature of the offences used to populate watchlists.

of the European Union, Joined Cases C-465/00, C-138/01 and C-139/01 Rechnungshof v Osterreichischer Rundfunk and Others, 20 May 2003, para. 71.

[129] *Tele2 Sverige AB v Post-och telestyrelsen* and *Secretary of State for the Home Department v. Watson and others*, Judgment, Grand Chamber, Court of Justice of the European Union, Cases C-203/15, C-698/15, 21 December 2016, para. 115. See also, *Zakharov v. Russia*, Judgment, ECtHR, App. No. 47143/06, 4 December 2015, para. 232.

[130] For instance, whether LFR is deployed at border ports or in general public spaces, or whether LFR is deployed as part of an isolated or interconnected system.

3. The Pre-Test Deployment Planning Phase

Before live test deployments of LFR technology are begun, a number of issues should be addressed. This section addresses the pre-test deployment preparation and planning phase. It focuses on: the nature of the LFR test deployments and the establishment of an appropriate methodology, the identification of an appropriate legal basis, the preparation of impact assessments, and public facing transparency.

It is emphasised that legal requirements, including the identification of an appropriate legal basis and measures to ensure human rights law compliance, should be undertaken in the pre-trial planning phase. This will facilitate the development of an appropriate methodology capable of ensuring compliance with relevant legal obligations.

3.1. The Nature of the Test Deployments Undertaken by the MPS and the Development of an Appropriate Methodology

This section addresses the nature of the LFR test deployments undertaken by the MPS, and in particular the fact that LFR technology was trialled during live operational deployments.[131] This discussion does not address the methodological basis for the MPS' scientific evaluation of face recognition, or the technical aspects of the test deployments. The focus herein is on the overall process, and whether the LFR test deployments were conducted in such a way that they could inform future police decision making relating to LFR.

The LFR test deployments offered a potentially valuable research opportunity to fill the significant gap in evidence with respect to the effectiveness and reliability of biometric/facial images for policing purposes.[132] In this regard, the test deployments offered an opportunity to both examine technical accuracy and to understand the implications of LFR on police operations. This point has been asserted in public statements made by a number of individuals holding governance and oversight roles, such as the Surveillance Camera Commissioner and the Biometrics Commissioner. For example, the Biometrics Commissioner's Annual Report for 2017 stated that:

> what needs to be understood is not just the matching capabilities of the software products but what kind of management and decision making system is required for such a police use in the criminal justice system.[133]

[131] The specific process adopted by the MPS is discussed above in Section 1.2.3.
[132] See section 1.2.3.
[133] Office of the Biometrics Commissioner (2018) 2017 Annual Report, London: HMSO para 308, p 88.

The question arises, however, as to whether the process surrounding the test deployments was developed in a manner capable of achieving these objectives. The authors have significant concerns in this regard.

The Metropolitan Police Service LFR deployments were regularly characterised as 'tests' or 'trials'. There are many general statements along these lines such as the illustrative, 'this operation is a trial to assess the reliability and effectiveness of LFR technology and methodology for a proportionate and necessary policing purpose'.[134] However, a review of the documents made available to the authors results in the clear conclusion that the LFR test deployments were not set up solely and specifically as a research initiative. Instead, the decision was made to trial LFR technology during operational deployments. While there may be valid reasons for adopting this approach, doing so necessarily required the development of a specific methodology in order to ensure a reliable process, capable of satisfying the purposes of the trial.

The 'MPS Live Facial Recognition Trial Evaluation Methodology' given to the authors states that:

> Metropolitan Police Service (MPS) has an objective to trial Live Facial Recognition (LFR) Technology in order to understand its potential as a tool for operational policing … The trial aims to provide an evidence base for strategic decision making as to the potential effectiveness of LFR as a policing tool and to determine:
>
> a) The performance that can be anticipated in operational LFR deployments
> b) The factors that significantly influence LFR performance
> c) Identify any desirable functionality that is missing from the current face recognition solution that would improve the system in terms of technical performance or ease of operation[135]

This methodology document focuses primarily on the technical aspects of the trials. There does not appear to be a clearly defined research plan that sets out how the test deployments are intended to satisfy the non-technical objectives, such as those relating to the utility of LFR as a policing tool. This necessarily complicated the trial process, and affected their effectiveness and overall utility.[136] This holds true with respect to other documentation prepared by the MPS. Although a number of

[134] 'Data Protection Impact Assessment for the use of Live Facial recognition within the MPS', 23 July 2018.
[135] 'MPS Live Facial Recognition Trial Evaluation Methodology' p 2.
[136] It is important to note that sound methodological reasons may exist for testing policing aims through an evaluation of technology. In addition, it is legitimate for the MPS to incorporate a number of open ended research questions to accommodate unanticipated issues as they arise during the research. However, these methodological choices also hold a range of implications explored below.

strategic intentions and operational objectives are elaborated on, it is unclear how they were to be evaluated.

Some of the problematics arising in this regard are demonstrated by the absence of a clear distinction between research objectives and possible measures of success from policing objectives. For example, the MPS Legal Mandate document speaks of 'identify[ing] and evaluat[ing] an *evidence base* from which the overt use and deployment of LFR technology will lead to a comprehensive assessment of LFR as a policing tactic' (emphasis added).[137] In the July 2018 Data Protection Impact Assessment the nature of this evidence base is somewhat indicated by reference to personal data, where it states:

> All personal data used is essential for the project and future deployment. Personal data is required to provide an evidential base in respect of evaluating the conditions and environment under which LFR can be deployed as a policing tactic.[138]

These research-specific terms are repeatedly interspersed with lists of policing aims for the deployments, such as 'to use LFR technology to reduce and disrupt crime and to increase enforcement opportunities at selected events' and 'to provide reassurance to communities at the selected events that the MPS are utilising innovative and effective approaches to policing.'[139] Frequently they are combined, for example in the MPS Legal Mandate's necessity analysis:

> It is necessary to conduct the trials in line with the strategic intentions, operational and technical objectives and to conduct a comprehensive evaluation (internal and external). This will contribute to the understanding of the overt use of LFR and how it presents a viable policing tactic.

Although a clear plan appeared to be in place to evaluate the technical performance of LFR technology, it is not clear how the assessment of LFR as a policing tactic was to be conducted. In the apparent absence of relevant clear objectives and markers of success to inform the test deployments, ensuring robust results is difficult. For example, it is unclear how the manner in which the test deployments were conducted could contribute to answer questions such as the impact of LFR on communities, or how LFR could be effectively incorporated into policing activities.

---

[137] 'Live Facial Recognition, (LFR) MPS Legal Mandate', 23 July 2018, p. 3.
[138] 'Data Protection Impact Assessment for the use of Live Facial recognition within the MPS', 23 July 2018, p. 11.
[139] 'Live Facial Recognition, (LFR) MPS Legal Mandate', 23 July 2018, p. 4. In addition, the aim of community reassurance does not appear to have been measured as part of the test deployments (see Section 3.1).

3.2.The Identification of an Appropriate Legal Basis 'In Accordance with the Law'

Before LFR technology can be trialled by the police in operational deployments, the legal basis underpinning its use must be clarified. The human rights law considerations relevant in this regard are outlined above.[140]

The MPS' understanding as to the legal basis underpinning the deployment of LFR technology is set out in a number of documents. The first such document obtained by the authors of this report is titled 'Live Facial Recognition, (LFR) MPS Legal Mandate' and is dated 23 July 2018.[141]

Before examining the legal mandate itself, it must be noted that the date of this document is of concern. The first trial was undertaken in August 2016, and a total of five test deployments were conducted prior to the publication of this document. It is not clear if this mandate is the first of its kind or an updated version of a previous document. If no legal basis was identified prior to the test deployments, it would have been impossible for the police to ensure the legality of those test deployments, and to provide legal justification for their activities. As such, they are likely to have constituted an arbitrary interference with individuals' rights and may be found to be unlawful on this basis.[142]

No one piece of legislation exists that explicitly authorises police use of LFR technology.[143] The legal mandate prepared by the MPS accordingly references a number of different sources of law in relation to (a) the authorisation of, and (b) the subsequent regulation of, LFR technology. These are:

- Common law
- Human Rights Act 1998
- Freedom of Information Act 2000
- Protection of Freedoms Act 2012, and
- Data Protection Act 2018.[144]
- Regulation of Investigatory Powers Act.[145]

Of the different legal frameworks identified by the MPS and discussed in the legal mandate document, only the common law and the Protection of Freedoms Act 2012

[140] See Section 2.2.1.
[141] This is available on the website of the Metropolitan Police Service: https://www.met.police.uk/SysSiteAssets/media/downloads/met/advice/lfr/live-facial-recognition-lfr-mps-legal-mandate.pdf. Last accessed 5 April 2019.
[142] See in particular, Section 2.2.1 above.
[143] Compare with the Investigatory Powers Act 2016, which provides explicit authorisation for a number of surveillance techniques.
[144] 'Live Facial Recognition, (LFR) MPS Legal Mandate', 23 July 2018, p. 4.
[145] This was added to the legal mandate in 2019, see 'Live Facial Recognition, (LFR) Operational Mandate), 16 January 2019, p. 4.

provide potential *implicit* authorisation for the deployment of LFR technology. The other sources either relate to public access to information regarding police activity – e.g. the Freedom of Information Act 2000 – or regulate the use of LFR technology, without establishing explicit legal authorisation for its use as such, e.g. the Human Rights Act 1998 and the Data Protection Act 2018.[146] Accordingly, in order to ensure that the 'in accordance with the law' requirement established under human rights law is satisfied, implicit authorisation under the common law, or potentially the Protection of Freedoms Act 2012, must be examined.

As stated in the MPS' legal mandate document, under common law:

> The police can, in fulfilling its operational duties, conduct themselves in a manner which is not contrary to law. These core principles are outlined below:
>
> - Protecting life and property.
> - Preserving order.
> - Preventing the commission of offences.
> - Bringing offenders to justice.[147]

Although explicit legal authorisation for the use of LFR technology cannot be found in the common law, the MPS may argue that an implicit legal basis exists as the use of LFR technology can contribute to the achievement of the four core principles elaborated above.

The operational mandate document written by the MPS also refers to Section 33 (subsections 1-4) of the Protection of Freedoms Act 2012.[148] This provision, however, refers to the application of the Surveillance Camera Commissioners Code. As such, it principally regulates the circumstances in which CCTV technology may be used for surveillance purposes.[149] It does not establish explicit authorisation for the deployment of LFR technology, although the MPS may argue that it creates an implicit legal basis.

The difficulty with relying upon the common law or the Protection of Freedoms Act 2012 as sources of implicit legal authorisation vis-à-vis the use of LFR technology is the ambiguity that will inevitably arise. It is recalled that the 'in accordance with the law' test established under human rights law incorporates a number of different

[146] For instance, as discussed above in Section 2.2.1, the Human Rights Act requires that a legal basis for any interference with rights be established. It does not itself establish that legal basis. The use of LFR technology is also discussed in the Surveillance Camera Commissioner's Code of Practice, which regulates issues relating to the deployment of LFR. See, for instance, Surveillance Camera Code of Practice, June 2013, sections 3.2.3, 4.8.1, 4.12.1.

[147] 'Live Facial Recognition, (LFR) MPS Legal Mandate', 23 July 2018, p. 5.

[148] 'Live Facial Recognition, (LFR) Operational Mandate', 16 January 2019, p. 7. A related document, named 'legal mandate', contains similar references vis-a-vis the legal basis. See, 'Live Facial Recognition, (LFR) Legal Mandate', 23 July 2018, p. 8.

[149] For instance, the Surveillance Camera Commissioner states that 'A legal framework exists which lends itself to the *operation* of surveillance camera systems'. Emphasis added.

elements, relating both to the existence of a legal basis and the quality of that legal basis. Key in this regard is the protection against arbitrary rights interferences, and the foreseeability of the law.[150]

Reference to existing case law reinforces the concern that the specific legal basis identified for the use of LFR technology may be overly ambiguous. For instance, in *S and Marper v. the United Kingdom*, the European Court of Human Rights noted that the objective of prevention or detection of crime 'is worded in rather general terms and may give rise to extensive interpretation'.[151] Similarly, in *Catt v. the United Kingdom*, which related to the collection of intelligence concerning domestic extremism, the European Court of Human Rights noted that:

> In light of the general nature of the police powers and the variety of definitions of the term "domestic extremism", the Court considers that there was significant ambiguity over the criteria being used by the police to govern the collection of the data in question. It notes that perhaps as a result, the database in issue appears to have been assembled on a somewhat *ad hoc* basis. The Court therefore agrees with the applicant that from the information available it is difficult to determine the exact scope and content of the data being collected and compiled to form the database.[152]

The Court further stated that: '[i]t is of concern that the collection of data for the purposes of the database did not have a clearer and more coherent legal base'.[153] At the domestic level, it was held in *R (Catt) v. Commissioner of Police of the Metropolis and another*, that:

> At common law the police have the power to obtain and store information for policing purposes, ie broadly speaking for the maintenance of public order and the prevention and detection of crime. These powers do not authorise intrusive methods of obtaining information[154]

The decision in *P.G. and J.H. v. the United Kingdom* concerned the use of covert surveillance technology, and is therefore distinct from the overt use of LFR technology, but the findings may nonetheless be relevant.[155] The key similarity relates to the ambiguity of the underlying legal basis, while it must also be recognised that although LFR is an overt technology it is particularly invasive and the potential for

[150] See above Section 2.2.1.
[151] *S. and Marper v. the United Kingdom*, Judgment, ECtHR, App. Nos. 30562/04 & 30566/04, 4 December 2008, para. 99.
[152] *Catt v. the United Kingdom,* Judgment, ECtHR, App. No. 43514/15, 24 January 2019, para. 97.
[153] *Catt v. the United Kingdom,* Judgment, ECtHR, App. No. 43514/15, 24 January 2019, para. 99.
[154] *R (Catt) v. Commissioner of Police of the Metropolis and another* [2015] UKSC 9, para 7 (Lord Sumpton).
[155] See, in this regard, *Catt v. the United Kingdom,* Judgment, ECtHR, App. No. 43514/15, 24 January 2019, para. 114.

rights interference extends beyond that typically associated with overt technologies. The Court stated that:

> While it may be permissible to rely on the implied powers of police officers to note evidence and collect and store exhibits for steps taken in the course of an investigation, it is trite law that specific statutory or other express legal authority is required for more invasive measures, whether searching private property or taking personal body samples. The Court has found that the lack of any express basis in law for the interception of telephone calls on public and private telephone systems and for using covert surveillance devices on private premises does not conform with the requirement of lawfulness […] The underlying principle that domestic law should provide protection against arbitrariness and abuse in the use of covert surveillance techniques applies equally in that situation.[156]

In considering the extension of reasoning related to covert powers to overt LFR technology, the finding in *Catt v. the United Kingdom* is relevant: '[u]nlike the present case, those cases dealt with covert surveillance. However, the Court considers it should be guided by this approach especially where it has already highlighted concerns relating to the ambiguity of the state's powers in this domain'.[157] The appropriateness of using certain elements associated with covert powers to guide the use of particular over technologies is underlined by reference to the MPS' acknowledgement that, although not directly applicable, the Regulation of Investigatory Powers Act 2000 should guide the use of LFR technology,[158] presumably on the basis of the level of intrusiveness involved in LFR.

Similar concerns regarding the ambiguity of the legal basis have been raised in academic commentary and in interviews conducted for the purposes of this report. For instance, in an interview conducted for this report Big Brother Watch stated that: '[t]here is a clear absence of legal basis'.[159] Such concerns were picked up by Purshouse and Campbell:

> One criticism of the FRT [Facial Recognition Technology] trials is that they have been operating in a legal vacuum. FRT is said to have no legal basis regulating its proper operational limits. The Home Office has responded to such concerns, claiming that three legal regimes have regulated the trials: the Data Protection Act 2018 (DAP 2018); the Surveillance Camera Code of Practice; and, relevant human rights

[156] *P.G. and J.H. v. the United Kingdom*, Judgment, ECtHR, App. No. 44787/98, 25 September 2001, para. 62.
[157] *Catt v. the United Kingdom,* Judgment, ECtHR, App. No. 43514/15, 24 January 2019, para. 114.
[158] 'Live Facial Recognition, (LFR) Operational Mandate), 16 January 2019, p. 4.
[159] Interview with Silkie Carlo, Director, Big Brother Watch.

> principles. However, none of these regimes provide guidelines or rules specifically regulating the police use of FRT. Moreover, in its recent Biometrics Strategy, the Home Office acknowledged that the governance and oversight of FRT surveillance could be "strengthened further".[160]

In an interview conducted for this report the Information Commissioner's Office noted that it is 'aware of concerns that there is no specific statutory framework for AFR (and other 'new' technologies)',[161] while the Surveillance Camera Commissioner noted that:

> [u]nlike ANPR, there are no national standards in place regarding AFR and central co-ordination with the NPCC is still evolving. The Home Office has at last delivered a Biometrics Strategy but there is much work to do. The state is in the foothills of persuading the public that there is a sufficiently robust regulatory regime in place to provide public reassurance.[162]

Emphasising this concern Liberty stated that:

> It's been very difficult to get a straight answer from the police about what they consider to be the legal basis, so it's difficult for me to give you a proper analysis, but suffice to say we haven't heard anything thus far that would make us believe that there is a legal basis. It wouldn't be appropriate, we don't think, or just accurate to draw on pre-existing legislation and essentially try and create a Venn Diagram of it all where at the point of overlap we say in this area somehow, it's giving us permission to use facial recognition or it's giving us a legal basis and protecting from the harms that we discussed.[163]

The implicit legal authorisation claimed by the MPS for the use of LFR appears inadequate when compared with the 'in accordance with the law' requirement established under human rights law. The absence of publicly available frameworks

---

[160] Joe Purshouse & Liz Campbell, 'Privacy, crime control and police use of automated facial recognition technology' (2019) Criminal Law Review 3, p. 198.

[161] Written response to questions, Information Commissioner's Office.

[162] Surveillance Camera Commissioner, Annual Report 2017-18, p. 35. The Home Office Biometrics Strategy was published on 28 June 2018, between the fifth and sixth Metropolitan Police LFR deployments. In a further indication of uncertainty in the regulatory landscape, while giving evidence to the House of Commons Science and Technology Committee during March 2019 the Biometrics Commissioner, Professor Paul Wiles, publicly criticised the strategy as a missed opportunity to provide regulatory clarity. He described the Home Office Biometrics Strategy as,

> a slightly confusing and disappointing document [that] starts off with what I might describe as a very good prologue for a strategy. It then simply becomes a list of some of, but by no means all, the things that the Home Office is doing on the use of biometrics—and then stops. I thought that that was disappointing. It was a missed opportunity to lay out a strategy (House of Commons Science and Technology Committee, 'Oral evidence: Work of the Biometrics Commissioner and the Forensic Science Regulator, HC 1970' Tuesday 19 March 2019).

[163] Interview with Hannah Couchman, Advocacy and Policy Officer, Liberty.

clearly circumscribing its circumstances of use – thereby facilitating foreseeability – reinforces this point.[164] Without explicit legal authorisation in domestic law it is highly possible that police deployment of LFR technology – as a particularly invasive surveillance technology directly affecting a number of human rights protections, including those relevant to democratic participation – may be held unlawful if challenged before the courts.

3.3. Efforts Undertaken to Meet the 'Necessary in a Democratic Society' Test

Impact or risk assessments should be conducted prior to the deployment of new technologies such as LFR in order to identify and understand any potential human rights harm.[165] These assessments are essential to determining whether the deployment may be considered 'necessary in a democratic society'.[166] This is confirmed in the Surveillance Camera Commissioner's recent guidance on 'Police Use of Automated Facial Recognition Technology with Surveillance Camera Systems'.[167]

The impact/risk assessments conducted by the MPS are contained in two core documents: 'Live Facial Recognition, (LFR) MPS Legal Mandate'[168] and 'Metropolitan Police Service Privacy Impact Assessment: Data Protection Impact Assessment for the Use of Live Facial Recognition within the MPS'.[169] The 'Privacy Impact Assessment for the use of facial imaging deployment at Terminal 1, King George Dock, Hull' prepared by Humberside Police and published following a freedom of information request makes reference to a Privacy Impact Assessment prepared by the MPS and dated 1 April 2016.[170] This latter document has not been seen by the authors.

---

[164] Case law concerning how guidance published on line can contribute to the 'foreseeability' requirement is discussed further above Section 2.2.1.
[165] See discussion above in Section 2.1.
[166] See above Section 2.2.3.
[167] See, Surveillance Camera Commissioner, 'Police Use of Automated Facial Recognition Technology with Surveillance Camera Systems: Section 33 Protection of Freedoms Act 2012', March 2019, pp. 3, 9.
[168] 'Live Facial Recognition, (LFR) MPS Legal Mandate', 23 July 2018.
[169] 'Data Protection Impact Assessment for the use of Live Facial recognition within the MPS', 25 July 2018; Metropolitan Police Service Privacy Impact Assessment: Data Protection Impact Assessment for the use of Live Facial recognition within the MPS, 12 February 2019. It is worth noting that a Freedom of Information request was made to the Metropolitan Police to provide their Privacy Impact Assessment (the forerunner to the Data Protection Impact Assessment) for the 2017 Remembrance Sunday test deployment. In response, the Metropolitan Police Service cited *Freedom of Information Act* 2000 Section 22(1) ((a) information Intended for Future) and declined to publish the assessment on the grounds that 'The PIA is currently being reviewed and updated and is still due to be published in the second quarter of 2018' (full correspondence available at https://www.whatdotheyknow.com/request/facial_recognition_used_on_the_r). Mention of 'updating' the PIA several months after the deployment is significant and the researchers have not been able to locate this document through online searches of web-based documentation.
[170] Humberside Police, 'Privacy Impact Assessment for the use of facial imaging deployment at Terminal 1, King George Dock, Hull', 12 June 2018, Freedom of Information Request Ref No: F-2018-01558.

No MPS documents have been seen that clearly set out the justification underpinning the deployment of LFR technology in a manner capable of addressing whether such deployments may be considered 'necessary in a democratic society'. Of particular concern is the lack of effective consideration of alternative measures, the absence of clear criteria for inclusion on the watchlist, including with respect to the seriousness of the underlying offence, and the failure to conduct an effective necessity and proportionality analysis.[171] For these reasons, and as discussed in greater detail in Sections 3.3.1 and 3.3.2, it is considered highly possible that the MPS's test deployments of LFR technology would not be regarded as 'necessary in a democratic society' if challenged before the courts.

As regards the MPS' approach to the necessity analysis,[172] two key inter-related issues may be highlighted: the classification of LFR technology as non-intrusive, and the narrow scope of the proportionality analysis. The content of the watchlist also has an impact on the necessity test, and the necessity test will need to be re-examined should the criteria used to populate the watchlist change. Issues to do with proportionality will be subsumed within this evaluation, in line with the discussion above.[173]

3.3.1. Watchlist Formulation and the Necessity Test

The content of the watchlist will impact upon the necessity analysis. This is demonstrated by the discussion above regarding the retention of custody images. Here, a distinction is drawn – in terms of the necessity, and therefore human rights compliance, of retention – between images relating to individuals convicted of an offence, and those who may have been detained, questioned, or prosecuted, but not convicted.[174] This issue appears directly relevant to watchlist formulation given the different categories of persons reportedly included on the watchlist, which apparently ranges from those wanted by the courts to those wanted for questioning, across a range of different offences. For instance, the MPS established that intended circumstances of use for LFR included the following:

> **LFR is intended to be utilised in the following applications:**
>
> · **To identify individuals shown as wanted by the police and the courts.**
>
> The MPS are seeking to deploy LFR in order to identify individuals who are shown as wanted by the police and criminal justice systems. The utilisation of LFR will assist in the

[171] The seriousness of the offence has been a key issue in case law relating to other forms of surveillance, such as the necessity of bulk communications surveillance. See, for example, *Tele2 Sverige AB v Post-och telestyrelsen* and *Secretary of State for the Home Department v. Watson and others*, Judgment, Grand Chamber, European Court of Justice, Cases C-203/15, C-698/15, 21 December 2016, para. 102; and *Szabo and Vissy v. Hungary*, Judgment, European Court of Human Rights, Application No. 37138/14, 12 January 2016, para. 73.

[172] As contained in the Data Protection Impact Assessment and MPS Legal Mandate documents.

[173] See Section 2.2.3.

[174] See above Section 2.2.3.

identification of offenders, thereby expediting their passage through the criminal justice system and therefore reducing the probability of repeat offending. The application of this technology will provide a more efficient and less intrusive means to identify and arrest wanted individuals in public spaces.

- **To identify individuals who present a risk of harm to themselves and others.**

LFR can provide event Commanders with an additional tactical option to enhance police capability within an operational policing footprint. This can be used to address a traditional crime issue, or reduce the risk of physical harm or violence through an intelligence based watch-list. This itself is focused on wanted individuals or identified individuals who may be drawn to an event who may cause safety implications for an event or themselves.

- **To support ongoing policing activity with regards to a specific problem or location.**

LFR can provide an additional asset to enhance a police response to address a particular issue, such as an increase of a specific crime type within a particular area. This will consist of a bespoke watch-list of wanted individuals or those with conditions not to attend an area based on intelligence and crime analysis.

- **To assist police in identifying individuals who may be at risk or vulnerable.**

LFR has the potential to be used to identify individuals who are believed to be vulnerable, missing, or suffering from mental health issues and at risk of harm.[175]

This was repeated in a subsequent document dated 12 February 2019, with the added caveat that the latter three categories were not being trialled at the time.[176] However, reports indicate that that these categories were included in at least some test deployments prior to the February 2019 document. For instance, Big Brother Watch report that the watchlist for the Remembrance Sunday trial was populated with a list of 'fixated individuals', not wanted in relation to any particular crime.[177] This was not denied by the MPS in their response to a Freedom of Information Request.[178] Although not specified, 'fixated individuals' presumably relates to either individual at risk or vulnerable, or individuals who present a risk of harm to themselves or others.

Ambiguity exists regarding the meaning of the terms used by the MPS to delimit LFR applications. For instance, the 'individuals shown as wanted by the police and the courts'[179] category is left largely unspecified in the July 2018 Data Protection

[175] See, 'Data Protection Impact Assessment for the use of Live Facial recognition within the MPS', 12 December 2018, p. 2.
[176] See, 'Data Protection Impact Assessment for the use of Live Facial recognition within the MPS', 12 February 2019, p. 2.
[177] Big Brother Watch, 'FaceOff: The lawless growth of facial recognition in UK policing', May 2018, p. 27.
[178] Freedom of Information Request Reference No: 2018030000548. Available at: https://bigbrotherwatch.org.uk/wp-content/uploads/2018/04/Metropolitan-Police-2018030000548.pdf. Last accessed 5 April 2019.
[179] DPIA July 2018: "The MPS are seeking to deploy LFR in order to identify individuals who are shown as wanted by the police and criminal justice systems. The utilisation of LFR will assist in the identification of offenders, thereby expediting their

Impact Assessment. No mention is made regarding the level of seriousness of the underlying offence or any other risk posed by the individual. Uncertainty also exists over what is meant by 'wanted'. This lack of specificity is significant to conducting the required necessity and proportionality assessment, and also raises issues regarding the legal basis requirement.[180]

An assumption might be made that 'wanted by the police and courts' indicates the existence of an outstanding arrest warrant. For instance, if an individual has failed to attend court as a defendant, has 'skipped bail' after being charged with an offence, or has perhaps even escaped from prison. These examples cover situations where formal judicial proceedings are in progress or where sufficient evidence exists to charge an individual. An arrest warrant may also be issued for individuals wanted for questioning. As this requires court authorisation, this will also require the provision of a sufficient level of information for a warrant to be granted.[181]

The above circumstances largely conform with most commonly-held understandings of what is meant by 'wanted'. They also correspond to the Humberside Privacy Impact Assessment (made in connection with the joint Humberside—MPS LFR trial of 13-14 June 2018): *'Wanted on warrant* means the individual is circulated on the Police National Computer (PNC[182]) after a court has issued a warrant for the police to arrest an individual'.[183]

However, the Humberside Privacy Impact Assessment also includes a second category of 'wanted':

> *Wanted by police* refers to individuals who are suspected of a crime and have been circulated as wanted on Police National Computer after an inspector has reviewed the case and satisfied themselves that the individual should be arrested in the interests of detecting and preventing crime.[184]

It might be surprising to the general public that the term 'wanted' may include 'wanted by the police', and may therefore include individuals without an outstanding arrest warrant.

---

passage through the criminal justice system and therefore reducing the probability of repeat offending. The application of this technology will provide a more efficient and less intrusive means to identify and arrest wanted individuals in public spaces"

[180] This is particularly true with respect to the prohibition of arbitrary rights interference, and the foreseeability requirement. See, Section 2.2.1.

[181] Of course, arrest warrants may be issued for many other matters, but these could be called the core purposes.

[182] The Police National Computer was established in 1974. It holds formal records of encounters of individuals with the police and other criminal justice agencies. For example, it holds data on arrests, charges, court decisions and a range of licensing records (such as driving and firearms).

[183] Humberside Police, 'Privacy Impact Assessment for the use of facial imaging deployment at Terminal 1, King George Dock, Hull', 12 June 2018, Freedom of Information Request Ref No: F-2018-01558.

[184] Humberside Police, 'Privacy Impact Assessment for the use of facial imaging deployment at Terminal 1, King George Dock, Hull', 12 June 2018, Freedom of Information Request Ref No: F-2018-01558.

Humberside Police have made publicly available their policy (as of 2018) on 'wanted persons' in respect to circulation on the Police National Computer.[185] Their definition of 'suspect' includes: "1. Where a victim names an offender they should be added as a suspect; 2. Where a witness names an offender to a police officer they should be added as a suspect". Circulation decisions are apparently scaled by reference to the Office for National Statistics Crime Severity Score.

It is not known whether other forces, notably the MPS, adopt the same approach. A Freedom of Information request in 2016 appears to remain unanswered.[186] In the absence of a definition, 'wanted by the police' may refer to a wide variety of individuals, at significantly varying levels of suspicion. For example, Crime Reporting Information System (CRIS)[187] reports are simply reported and unfiltered victim statements and witness statements pertaining to reported criminal incidents.

In short, there are two elements at stake here: (1) type and seriousness of the offences deemed suitable for watchlist selection and (2) whether the individual is wanted on warrant (of the type specified above) or merely 'wanted by the police', even when this is based on low level intelligence. Similar issues of ambiguity and the absence of an evidential threshold are also relevant to the three other criteria identified in the Data Protection Impact Assessments.[188]

The European Court of Human Rights case law regarding custody images, finger prints, and DNA samples,[189] indicates that there are clear differences between the categories of persons potentially included on the watchlist. The nature of the offence warranting inclusion on the watchlist (i.e. its level of seriousness) will also inform the necessity analysis. The necessity of using LFR technology to identify different categories of individuals will accordingly differ. Two issues emerge. First, in light of the distinctions between different categories of persons, and on the basis of the longstanding case law, it appears inappropriate that the MPS include all categories of persons within the same necessity analysis: distinct analysis is likely to be required. Second, as the necessity analysis is dependent upon the content of the watchlist, a fresh necessity analysis should be conducted each time the criteria used to formulate

---

[185] Humberside Police, Policy and Procedure: Wanted Persons, 26.04.2018 (not protectively marked) https://www.humberside.police.uk/sites/default/files/Wanted%20Persons%20V12.4.pdf

[186] Freedom of Information Request Reference No: 2016050000848, 22.5. 2016.
"[...] Could the MPS clarify whether in any other situation other than those mentioned above [arrest warrants], an individual who needs to be arrested/is wanted (e.g. for failing to appear at a police station, for which the police have the power of arrest without warrant under sec. 46A of PACE) is simply circulated as 'wanted' (or another marker) on the PNC, instead of having an 'arrest warrant' for them? [....]In other words, could the MPS specify under which situations an 'arrest warrant' (of either type) is issued, and under which other situations an individual would be circulated [as wanted] on the PNC?"
Available at: https://www.whatdotheyknow.com/request/difference_between_being_circula.

[187] An MPS database for logging incidents. See section 4.2.

[188] These were 'to identify individuals who present a risk of harm to themselves and others', 'to support ongoing policing activity with regards to a specific problem or location', and 'to assist police in identifying individuals who may be at risk or vulnerable'.

[189] See above Section 2.2.3.

the watchlist is altered. It is unclear whether this occurred. Although no differences appear in the analysis across the different documents prepared by the MPS, it may be the case that fresh analysis was conducted but that the conclusion remained the same. The 'in accordance with the law' requirement also requires a degree of foreseeability. To this end clear criteria regarding those categories of individuals included on the watchlist should be made publicly available.[190]

This precision is important for two further reasons: First, a review of social media and other forums reveals considerable public speculation over the content of watchlists. This directly connects watchlist construction with the public legitimacy of LFR as a whole. Second, and relatedly, clarity, precision and transparency regarding the population of watchlists is related to the issues of consent for those walking past LFR cameras.[191]

Concern has also been raised regarding the source of the images used to populate the watchlist. In particular, there is concern that custody images of individuals not charged or convicted of a crime may be used.[192] Addressing this issue will bring into play the same human rights considerations discussed in Section 2.2.3.[193]

3.3.2. Classification of LFR Technology as 'Non-Intrusive' and the Narrow Scope of the Proportionality Analysis

The documentation prepared by the MPS consistently classifies the use of LFR technology as non-intrusive. For instance, the 14 February 2019 Operational Mandate states that: 'LFR provides a means of addressing reductions in the numbers of violent crimes and those wanted by police or courts for such crimes through overt means and does not rely on intrusive means to do so.'[194] A similar claim is made in the Data Protection Impact Assessment: 'Operations take place in a public place and are not 'intrusive' or 'covert' as defined under RIPA 2000.'[195] This conclusion is consistent with the definition of intrusive surveillance established under section 26 of the Regulation of Investigatory Powers Act 2000.[196]

However, based on a review of the MPS' legal analysis and subsequent reasoning, it appears that classification of LFR technology as non-intrusive has resulted in it being treated as benign. As such, there is a clear concern that the MPS did not take account of the specific nature of LFR technology and its increased capability when compared

[190] See above Section 2.2.1.
[191] See below Section 4.4.
[192] See, Big Brother Watch, 'Face Off: The lawless growth of facial recognition in UK policing', May 2018, p. 21; Liberty, 'Resist Facial Recognition' available at: https://www.libertyhumanrights.org.uk/resist-facial-recognition.
[193] See also, *RMC and FJ v. Commissioner of Police of the Metropolis* [2012] EWHC 1681 (Admin); Home Office, 'Review of the Use and Retention of Custody Images', 2017.
[194] 'Live Facial Recognition, (LFR) Operational Mandate), 16 January 2019, p. 5.
[195] 'Data Protection Impact Assessment for the use of Live Facial recognition within the MPS', 25 July 2018, p. 5.
[196] S.26, Regulation of Investigatory Powers Act 2000.

with other forms of overt surveillance, such as open street surveillance cameras. This narrower approach appears to have had the effect of closing down further analysis, meaning that the more intrusive features of LFR have not been held to sufficient scrutiny, potentially raising concerns in relation to human rights law compliance.

As noted above, the use of LFR technology gives rise to an interference with the right to privacy.[197] It may also interfere with other rights, such as the right to freedom of expression, and the right to freedom of assembly and association.[198] The extent of any interference in this regard will depend upon factors such as the nature of a specific deployment, and the content of the watchlist.[199] Accordingly, although LFR technology may be deployed in a public place, this technology is distinguished from more traditional forms of overt surveillance – such as the mere monitoring of a public space or protest by police officers or surveillance cameras – which may not give rise to a rights interference.[200] The distinct nature of LFR technology demands a more in-depth risk assessment. This is suggested in the Surveillance Camera Code of Practice: '[i]n general, any increase in the capability of surveillance camera system technology also has the potential to increase the likelihood of intrusion into an individual's privacy.'[201] Indeed, the MPS' decision that the Regulation of Investigatory Powers Act 2000 should guide the use of LFR technology[202] appears to be a clear acknowledgement of the increased intrusiveness of this technology.[203]

As LFR technology gives rise to rights interference(s) its deployment must be evaluated in order to ensure compliance with human rights law.[204] This requires engaging with the 'necessary in a democratic society' test. It does not appear possible to fully comply with this requirement if classification of LFR technology as non-intrusive has the effect of precluding further analysis. Although not discussed in any detail herein, data protection requirements should also be incorporated into this analysis. [check section 35(8) of DPA 2018]

This conclusion is reinforced by reference to the proportionality analysis conducted by the MPS. This analysis is inappropriately narrow, and fails to adequately take into account the impact that the deployment of LFR technology has on those individuals who do not appear on the watchlist but who are subject to data processing by the

[197] This is discussed further above in Section 2.1.1.
[198] This is discussed further above in Section 2.1.2.
[199] Relevant factors include whether LFR is deployed at a border crossing or in a public spaces, whether it interacts with other systems, whether imagery is subject to automatic analysis, and the different categories of persons used to populate the watchlist.
[200] This is discussed further in Section 2.1.1.
[201] 'Surveillance Camera Code of Practice Pursuant to Section 20 of the Protection of Freedoms Act 2012', Home Office, para 2.2.
[202] 'Live Facial Recognition, (LFR) Operational Mandate), 16 January 2019, p. 4
[203] See also, Surveillance Camera Commissioner, 'Police Use of Automated Facial Recognition Technology with Surveillance Camera Systems: Section 33 Protection of Freedoms Act 2012', March 2019, p. 3.
[204] See further, above, Section 0.

LFR technology,[205] or the impact on those individuals who are incorrectly identified as being on the watchlist (i.e. as a result of false positives). As the processing of individuals' data gives rise to a rights interference, the necessity of this interference must be justified, but the documentation provides inadequate consideration with respect to these individuals.[206] They are effectively excluded from the proportionality analysis, indicating that the overall rights impact of the technology is not taken into consideration. When interviewed for this research, MPS officers in specialist units highlighted how accepted police practices for identifying 'wanted' individuals necessarily involve a range of (often highly) intrusive measures. However, this claim (a) fails to take into account the distinct nature of LFR, and the fact that it subjects all individuals passing a particular public place to biometric processing, and (b) does not negate the need to justify the necessity of particular measures, as required by human rights law.

The need to conduct a broader proportionality analysis – one that also takes into account the rights impact of those not on the watchlist – is underlined by reference to police involvement in, and relevant responses to, the use of LFR technology in a Manchester shopping centre. In this instance it was concluded that the use of LFR technology was not proportionate, precisely because of the impact on uninvolved individuals.[207] This incident was publicised by the Surveillance Camera Commissioner on 10 December 2018.[208] In this situation the Greater Manchester Police ceased their involvement in the use of LFR technology.

3.4.Transparency

The Surveillance Camera Code of Practice states that:

> The government considers that wherever overt surveillance in public places is in pursuit of a legitimate aim and meets a pressing need, any such surveillance should be characterised as surveillance by consent, and such consent on the part of the community must be informed consent and not assumed by the system operator. […] It denotes that the legitimacy of policing in the eyes of the public is based upon a general

[205] This conclusion is discussed above, in Section 3.3.1, and is also shared by the Surveillance Camera Commissioner. See, Surveillance Camera Commissioner, 'Working together on automatic facial recognition', 10 October 2018. Available at: https://videosurveillance.blog.gov.uk/2018/10/10/working-together-on-automatic-facial-recognition/.

[206] The 'collateral intrusion' analysis conducted by the Metropolitan Police is similarly narrow, and fails to take into account factors such as the initial processing of all subjects data or the existence of false positives. See, 'Live Facial Recognition, (LFR) MPS Legal Mandate', 23 July 2018, p. 6.

[207] '[Compared to the size and scale of the processing of all people passing a camera the group they might hope to identify was miniscule.' See, Surveillance Camera Commissioner, 'Working together on automatic facial recognition', 10 October 2018. Available at: https://videosurveillance.blog.gov.uk/2018/10/10/working-together-on-automatic-facial-recognition/.

[208] Surveillance Camera Commissioner, 'Working together on automatic facial recognition', 10 October 2018. Available at: https://videosurveillance.blog.gov.uk/2018/10/10/working-together-on-automatic-facial-recognition/.

> consensus of support that follows from transparency about their powers, demonstrating integrity in exercising those power and their accountability for doing so.[209]

Specific requirements regarding transparency are elaborated on further, in subsequent sections of the Code of Practice:

> Surveillance by consent is dependent upon transparency and accountability on the part of a system operator. The provision of information is the first step to transparency, and is also a key mechanism of accountability. In the development or review of any surveillance camera system, proportionate consultation and engagement with the public and partners (including the police) will be an important part of assessing whether there is a legitimate aim and a pressing need and whether the system itself is a proportionate response. Such consultation and engagement also provides an opportunity to identify any concerns and modify the proposition to strike the most appropriate balance between public protection and individual privacy.[210]

In specific guidance regarding police use of live facial recognition technology, the Surveillance Camera Commissioner further stated that:

> Transparency and accountability on the part of a relevant authority are key elements of public interest when operating AFR in public places. Not only are these legislative requirements, they are essential contributing factors to engendering public trust and confidence in the operation of surveillance camera systems.[211]

The importance of transparency was also highlighted by the Surveillance Camera Commissioner, in an interview conducted for this report: 'there needs to be legitimacy in its [LFR technology] moving forward because it is seen as so invasive […] I think the organisations using it have to attain a higher trust.'[212]

This section will accordingly discuss transparency in relation to the availability of information regarding the deployments, and engagement with the broader community. This discussion is also significant in relation to the issue of consent as discussed in Section 4.4 below.

---

[209] Surveillance Camera Code of Practice Pursuant to Section 20 of the Protection of Freedoms Act 2012', Home Office, para. 1.5.
[210] Surveillance Camera Code of Practice Pursuant to Section 20 of the Protection of Freedoms Act 2012', Home Office, para. 3.3.2.
[211] Surveillance Camera Commissioner, 'Police Use of Automated Facial Recognition Technology with Surveillance Camera Systems: Section 33 Protection of Freedoms Act 2012', March 2019, p. 13.
[212] Interview with Tony Porter, Surveillance Camera Commissioner.

3.4.1. The Availability of Information Regarding Deployments

The first MPS documents obtained by the authors which provides information on the use of LFR technology are dated 23 and 25 July 2018.[213] From information available online, the MPS' LFR trial website – which contains information relating to the trial process, the legal mandate, and the data protection impact assessment – appears to have been created on 15 July 2018.[214] This indicates that no detailed information was available to the public prior to 15 July 2018 at the earliest. As the first trial was conducted in August 2016, and a total of five trials were conducted prior to 15 July 2018, this is clearly of concern with respect to the public availability of information, as required by the Surveillance Camera Commissioner's Code of Practice.

It is clear from observation of planning meetings that the public-facing website was developed in good faith, and motivated by a wish to engage the public and provide a measure of transparency, rather than servicing minimum regulatory requirements. This attitude was further demonstrated by a number of initiatives undertaken by key individuals within the MPS. For example, and as detailed in Section 4.2.4 below, Data Protection Impact Assessments were published on this website without any legal obligation to do so.[215] The decision to support this research also demonstrates an increased commitment to transparency and public engagement. Senior officers engaged in the planning of the test deployments established what they referred to as a 'stakeholder group' that included public opponents of live facial recognition. These included civil society groups, such as Liberty and Big Brother Watch, who were engaged in legal challenges against the use of LFR by the MPS and South Wales Police. Several additional meetings were held with these groups and there was a clear sense that senior planning officers encouraged this engagement. However, the effectiveness of this stakeholder group is unclear. For instance, in an interview conducted for the purposes of this report a representative of Liberty stated straightforwardly that: 'We don't consider ourselves part of that stakeholder group',[216] while a representative of Big Brother Watch noted that any engagement by the MPS was 'responsive rather than proactive.'[217]

Most test deployments observed by the authors included visits to the control room by regulators, interested politicians and others holding a review or oversight role. Technical and operational staff were available to answer visitors' questions and, in the authors' assessment, there was a clear sense of openness in the answers provided. On at least two occasions the technical team received unexpected visits from politicians requesting access to the control room. On both these occasions

[213] 'Live Facial Recognition, (LFR) MPS Legal Mandate', 23 July 2018; 'Data Protection Impact Assessment for the use of Live Facial recognition within the MPS', 25 July 2018.
[214] Available at: https://www.met.police.uk/live-facial-recognition-trial/.
[215] However, it is also relevant to note that key features of the website were not kept updated.
[216] Interview with Hannah Couchman, Advocacy and Policy Officer, Liberty.
[217] Interview with Silkie Carlo, Director, Big Brother Watch.

senior officers considered the request, deliberated issues of operational security, and granted access, with the knowledge that these individuals were vocal opponents of the technology, in the interests of pursuing transparency.

Following the creation of the website, and the publication of the legal mandate and the data protection impact assessment, a certain amount of information concerning the trials was available to the public as of July 2018.[218] Information was also made available with respect to specific deployments. For example, a Twitter presence was maintained and a press release was issued several days before each LFR test deployment during the period of observation (excluding the first Romford trial, when this was issued the day before). At pre-deployment planning meetings officers were clear that this strategy would allow critics of LFR more time to mobilise their opposition. The authors' observations of these meetings were that officers elected to issue these press releases in good faith, on the basis of better informing the public and in order to allow opposition groups to exercise their right to stage protests.

That said, the effectiveness of the measures may be questioned. A number of criticisms have been raised by those interviewed for this report regarding the extent to which the MPS made information available. For instance, Liberty noted that,

> from our perspective, we think there's a real lack of public understanding and public engagement. […] How you inform the public is important. Press releases aren't informing the public.[219]

Relatedly, representatives from the Information Commissioner's Office stated that:

> In the trials, the fair processing has included leafleting and signage around the van. The MPS published webpages with more information, towards the end of the trial, but it didn't always keep up with deployments.[220]

This frustration with the availability of information was evident, not only with respect to the test deployments, but also in relation to intended future use of LFR technology. As stated by Liberty:

> the police have been very reluctant, the police and the Home Office, have been very reluctant to engage with the question of how facial recognition links in with other technologies, other developments, other databases, so concerns about the new LEDS[221] database and how it might associate

[218] For discussion regarding this information, see above Section 3.2, and Section **Error! Reference source not found.**.
[219] Interview with Hannah Couchman, Advocacy and Policy Officer, Liberty.
[220] Written submission by the Information Commissioner's Office for this report.
[221] The Law Enforcement Data Service. This is the new Home Office driven data platform designed to replace the Police National Computer and Police National Database, see section 4.2.1.

> with that, concerns about where the photographs are coming from in the first place, how this might be used with body-worn video, how it might be used with CCTV.[222]

Overall, there is a sense that as the trials progressed there was a clear intention on the part of specific MPS staff to engage more widely and, at times, significant efforts were made to attempt this. However, there were significant shortcomings in relation to how this process was conducted. Equally, it is noted that this task fell to a small number of individuals and did not receive the infrastructural support necessary to be wholly effective. Moreover, this generated a tendency to combine the distinct activities of consultation and public engagement. Both are crucial to embedding standards of transparency and to building public confidence in policing and therefore require substantive institutional backing to enable their success.

A related issue concerns the sequence of any consultation. As noted above, the Surveillance Camera Commissioner's Code of Practice indicates that, prior to deployment, efforts should be made to engage with the broader public, in order to inform them of the purpose of the test deployments, to generate consent, and to obtain feedback. On our understanding, the broader public includes both members of the public and relevant civil society and non-governmental organisations. Any consultation should be 'meaningful and undertaken at a stage where there is a realistic prospect of influencing developments.'[223]

We are not aware that any broader public engagement with members of the public or relevant civil society and non-governmental organisations was undertaken prior to the initiation of the test deployments in 2016. This would appear to be inconsistent with the Surveillance Camera Commissioner's Code of Practice.

As noted above, efforts were made to engage with certain non-governmental organisations at later stages. This is an important development, and represents a valuable step towards transparency. Yet as noted by those civil society organisations: engagement with external groups did not occur at a stage in the process where feedback into how the deployments were run, or how the technology was used, could be incorporated.

3.4.2. Engaging the Broader Community

To our knowledge, beyond the measures outlined above, no further initiatives were undertaken to engage directly with members of the public resident in deployment areas, prior to deployment.

---

[222] Interview with Hannah Couchman, Advocacy and Policy Officer, Liberty.

[223] Surveillance Camera Code of Practice Pursuant to Section 20 of the Protection of Freedoms Act 2012', Home Office, para. 3.3.3.

As noted in Section 4, claims regarding the role of LFR technology in providing 'community reassurance' were repeatedly made during the Stratford test deployments. These claims were supported through reference to a 'Community Impact Assessment' that had been completed in advance. On further examination, however, planners revealed that the compilation of these community impact assessments did not involve direct engagement with the community. Moreover, they did not gather specific views on LFR technology. Instead, these assessments comprised a compilation of police-held statistics and general intelligence assessments of the area. In such circumstances, and in the absence of evidence, it is difficult to claim community support or public consent for the initiative.

While community engagement and measures of legitimacy and consent are relevant to all policing activities, the intrusive potential of facial recognition surveillance arguably places a greater requirement for securing trust and community approval. These different thresholds, and the approaches required to meet them, are acknowledged in other sensitive areas of policing. This point was articulated by the Surveillance Camera Commissioner when interviewed for this report, who contrasted the MPS approach to:

> consequence management in the world of counter terrorism policing operations. Because it was recognised from the get-go that there was amazing sensitivity with broad swathes of community... So what was put in place [in respect to counter-terrorism measures] was almost an in-depth checklist of key components of a community strategy. MPs, local councillors, business, people, residents in the area, communication that was evidenced and detailed. And was capable of gathering feedback. Prior to the deployment of a counter terrorism operation, there would be a time scale where these things would hit. I did say to the Met, you need to operate at that level of engagement as you would in a consequence management operation of a highly sensitive policing operation. Now, they may say they've done that. I haven't seen that rigorously evidenced, but they may have done that…
>
> I would have had the MPs, the councillors, I would have had civic leaders, I would have had resident association leaders, I would have had the businesses in the area. I would have had representatives of gangs and crimes, I would have had the high-profile groups, not just Liberty. I would have at least have let them know and I would have had tick lists. I would have let the Minister be aware [and the] Home Office … given its sensitivity, I think that was exactly what was required.[224]

[224] Interview with Tony Porter, Surveillance Camera Commissioner.

Upholding principles of 'surveillance by consent' is a requirement for less intrusive measures and therefore should be developed and enhanced for these more sensitive applications of technology.[225] Key to this is substantive and genuine public engagement.

[225] To date there has been one major study into the acceptability of LFR among Londoners. This was published by the London Police Ethics Panel in May 2019, after the conclusion of the MPS test deployments (London Police Ethics Panel (2019) *Final Report on Live Facial Recognition*, available from http://www.policingethicspanel.london/uploads/4/4/0/7/44076193/lfr_final_report_-_may_2019.pdf). This survey of 1,092 participants revealed that 57% of respondents considered police use of LFR was acceptable. This figure varied depending on participant's demographic position and the suggested use of LFR. For example, most participants under the age of 40 were not accepting of police uses of LFR (45% in the 16-24 age category and 48% in the 25-39 range), while those over 40 were more likely to deem police uses of the technology acceptable (62% of the 40-54 age range and 66% of those over 55 years old).

4. The Deployment Phase

4.1. Introduction

Section 4 of the report analyses the ways LFR worked in practice. This section draws on findings generated by qualitative social science observation and interview research methods.[226]

4.1.1. A Note on Terminology

A number of key terms are used throughout this discussion and are important to conveying the ways in which LFR works in practice:

- 'Adjudication' refers to the process of deliberation whereby officers assessed the credibility of a face recognition match. Computer-generated matches[227] of passers-by to watchlist records were judged as either credible or non-credible. If judged credible, the next step would normally be for intervention team officers to locate and question the individual concerned.
- 'Alert' and 'match' are used interchangeably. When the computer matches a camera image with a record on the database/watchlist it sends an 'alert' to officers.
- 'Control room' was the central location receiving camera feeds and alerts for LFR matches. In Stratford this was a static location. For all other trials the control room was accommodated in a mobile face recognition van.
- 'False positives' are erroneous matches. Typically, these occurred when a passer-by was wrongly matched to an individual on the LFR database (the 'watchlist'). This is defined in more detail below in section 4.1.3.
- 'Intelligence units' were specialist officers monitoring LFR feeds. They reviewed images in a 'control room'. On receiving an alert, the ideal process involved them judging the credibility of the computer-generated match (adjudication). If a match was deemed credible, the intelligence unit would instruct street-based police (intervention teams) to stop the subject.
- 'Intervention teams' were street-based police responsible for stopping individuals on the instruction of intelligence units.
- 'True positives' refer to instances when the system correctly identifies a passer-by to a corresponding record on the live facial recognition database (the 'watchlist'). This is defined in more detail below in section 4.1.3.
- 'Verified incorrect matches' are instances when a computer generated match is judged to be credible by a human operator yet proven incorrect following an identity check.

[226] The methodology adopted is discussed further in Section 1.1.
[227] Also known in the literature as 'computational matches'.

- 'Verified correct matches' are instances when a computer generated match is judged to be credible by a human operator and proven correct following an identity check.

'Watchlist' refers to the database of individuals against which live camera images were matched.[228]

4.1.2. Top Level Summary of Data

The MPS conducted 10 test deployments of LFR technology in London between 2016 and 2019. The authors became involved in the process part-way through and observed the final six of these. The test deployments were:

Table 4.1. MPS LFR Deployments Occurring Before Research commenced[229]

Trial	Date	Number of LFR matches	Watchlist size
Notting Hill Carnival 2016	28-29/08/2016	1	266
Notting Hill Carnival 2017	27-28/08/2017	96	528
Remembrance Sunday 2017	12/11/2017	7	42
Humberside Port 2018	13-14/06/2018	0	144

Table 4.2. Observed MPS LFR Deployments

Trial	Date	Number of LFR matches	Watchlist size
Stratford 1	28/6/2018	5	489
Stratford 2	26/7/2018	1	306
Soho 1	17/12/2018	5	2226
Soho 2	18/12/2018	9	2226
Romford 1	31/1/2019	10	2401
Romford 2	14/2/2019	16	1996

Overall, the LFR system generated 46 matches over the course of observed test deployments, involving 45 separate individuals.[230] Three of those matches are discounted from the analysis because they occurred before the street based intervention teams were deployed and, therefore, no capacity existed to attend to any

[228] In the literature on facial recognition, an image on the watchlist (reference database) is sometimes called a 'gallery image' while the imported image (in this instance, from the live camera feed) is called the 'probe image'.
[229] These test deployments were not observed by the research team; data was provided MPS facial recognition technical evaluation team.
[230] At the first Romford trial the same individual was matched twice at separate times in the same afternoon.

alerts. 42 matches are therefore included in the analysis that follows in this section. Unless explicitly stated otherwise, all data and discussion below focuses on the final six observed test deployments.

Table 4.3. Top Level Summary of LFR Matches and Adjudication Rates

Total number of individual cases where the LFR system matched an individual to a watchlist entry (and are eligible for analysis).	Individual cases conclusively **adjudicated as non-credible** by officers at all stages of the intervention process	Percentage of individual cases conclusively **adjudicated as non-credible** by officers during the intervention process
42	16[231]	38.1%

MPS officers considered the LFR match sufficiently credible to stop individuals and perform an identity check on 26 occasions. Four of these attempted interventions were unsuccessful. Usually this was because the individual became lost in a crowd. Of the remaining 22 stops, 14 were verified as incorrect matches following an identity check. Eight verified as correct matches following an identity check. This means that across all six observed trials, computer-generated face recognition matches were verifiably correct on eight occasions.[232]

Table 4.4 Numbers and Percentages of Correct and Incorrect Matches from Completed Identity Checks

Number of **attempts** to stop an individual following a computer-generated match adjudicated as credible	Number of individuals **stopped** for an identity check	Number of incorrect matches among individuals stopped for an identity check	Number of correct matches among individuals stopped for an identity check	Percentage of incorrect matches among individuals stopped for an identity check (14 of 22 stops)	Percentage of correct matches among individuals stopped for an identity check (8 of 22 stops)
26	22	14	8[233]	63.64%	36.36%

[231] First Soho test deployment, table 4.7., alerts: 3, 5. Second Soho test deployment, table 4.8., alerts: 1, 2, 3, 4, 6, 9. First Romford test deployment, table 4.9., alerts: 2, 10. Second Romford test deployment, table 4.10., alerts: 2, 5, 8, 9, 10, 15.

[232] This should not be interpreted as computer generated matches were *only* correct on eight occasions, but that they were only *verifiably correct* on eight occasions. Without checking the individual's identity it is impossible to know if a match adjudicated to be non-credible was a false positive.

[233] First Soho test deployment, table 4.7., alert 2. Second Soho test deployment, table 4.8., alert 5. First Romford test deployment, table 4.9., alerts: 5, 6, 7 (alert 8 excluded from the analysis due to double counting). Second Romford test deployment, table 4.10., alerts: 4, 11, 12.

Fig. 4.1. Verified Correct and Verified Incorrect LFR Matches Following Completed Police Interventions (*n*=22)

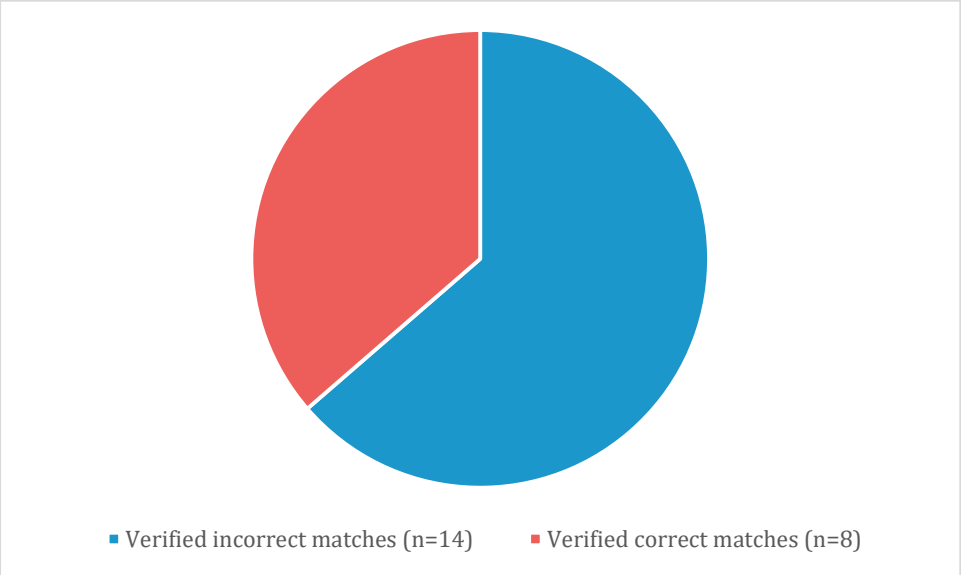
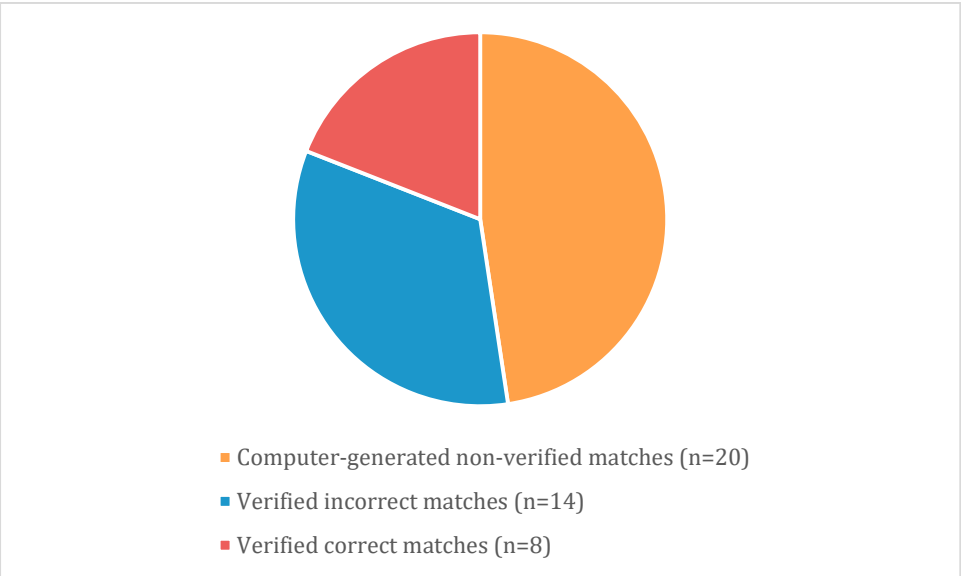


Fig 4.2. places this data in the context of the overall number of LFR matches occurring across the six test deployments. 42 alerts were generated that were eligible for the analysis. Of these, 20 were not be verified as correct or incorrect by an identity check. Some of these involve matches of individuals who became lose in the crowd (four cases). The majority of these 20 cases (16) concern matches that were adjudicated as not credible by the intelligence units in the control room. As such, no engagement with the matched individual took place and the match was not verified either as correct or incorrect.

Fig. 4.2. Non-verified, Verified Correct and Verified Incorrect LFR Matches (*n*=42 alerts eligible for analysis)



4.1.3. Issues Relating to LFR Performance Evaluation

This section raises certain problematics arising in relation to how LFR performance is evaluated. It looks first at issues regarding the number of matches generated compared to the overall size of the watchlist, and then raising issues with respect to the determination of false positives.

Matches v watchlist size

The size of the watchlists varied considerably across the observed test deployments.

As noted above, the LFR system generated 46 separate *alerts* over the course of observed test deployments. 45 separate *individuals* were matched to watchlist records; at the first Romford trial the same individual was matched twice at separate times in the afternoon.

Several different and potentially conflicting conclusions could be drawn from the headline data. Some planners argued that a larger watchlist would result in an increased number of matches. This reasoning was used on several occasions as an argument for substantial increases in watchlist size throughout the trial period.

However, making a judgement of system performance based on the size of a watchlist would depend on whether it was the *absolute number* of matches or a different measure, such as the *proportion of matches to watchlist size*, that was being counted. To illustrate, over the period of observation, the proportion of matches to watchlist size was highest at the first Stratford trial, despite the watchlist being comparatively smaller to that used in other test deployments. Interestingly, this trial was also the shortest of any of the observed deployments, leaving less available time for matches to be made.

Table 4.5. All LFR Alerts and Watchlist Sizes (Last Six Trial Deployments)

Trial	Date	Number of computer-generated LFR matches	Watchlist size	Ratio of LFR matches to watchlist size
Stratford 1	28/6/2018	5	489	1:97.80
Stratford 2	26/7/2018	1	306	1:306.00
Soho 1	17/12/2018	5	2226	1:445.20
Soho 2	18/12/2018	9	2226	1:247.33
Romford 1	31/1/2019	10	2401	1:240.10
Romford 2	14/2/2019	16	1996	1:124.75

While not observed by the research team, and therefore only included for illustrative purposes, data from the alerts generated at the first four test deployments further demonstrate the problems with drawing definitive conclusions from comparing watchlist size and number of alerts. This data is also not comparable with that presented in the previous table given the use of a different, and apparently less effective, face recognition algorithm during the first three deployments. The intention here is to illustrate the wide and unreliable variance in the ratio between alerts and watchlist size.

Table 4.6. All LFR Alerts and Watchlist Sizes (First Four Trial Deployments)[234]

Trial	Date	Number of computer generated LFR matches	Watchlist size	Ratio of LFR matches to watchlist size
Notting Hill Carnival 2016	28-29/08/2016	1	266	1:266.00
Notting Hill Carnival 2017	27-28/08/2017	96	528	1:5.50
Remembrance Sunday 2017	12/11/2017	7	42	1:6.00
Humberside Port 2018	13-14/06/2018	0	144	n/a due to n=0

Taken together, the evidence presented by the test deployments demonstrate the shortcomings of any conclusions over LFR effectiveness based on counting absolute numbers of matches. It is also important to recognise how such calculations, outcomes and ratios are influenced by a range of additional and unaccounted for variables. These include the time in which the cameras were active and the density of crowds passing the cameras. The MPS technological evaluation of the deployments has reportedly developed a methodology in this regard, accounting for and weighting the influence of many such variables.

Determining false positives

Dispute exists over the most accurate way to measure true and false positives in respect to LFR computational matches. This is reflected in the clashing statistical claims made about LFR. One widely cited claim is that 98% of police LFR matches made nationally were false positives.[235] This appears to have been calculated on the basis of comparing publicly available data on, and Freedom of Information requests for, the number of LFR computer-generated matches against numbers of ultimately true positives, that being the number of individuals whose identity was confirmed

[234] These trial deployments were not observed by the research team, data was provided by the MPS facial recognition technical evaluation team.

[235] Big Brother Watch, 'Face Off: The lawless growth of facial recognition in UK policing', 2018, p. 3.

on the ground. This methodology has been disputed by others evaluating the technology, who counter-claim that false positives should be calculated on the basis of comparing the *number of faces scanned* against the number of false alerts. This would yield a far lower percentage of false positives because the cameras normally scan many thousands of faces per hour as people pass their 'zone of recognition', and generate alerts comparatively rarely.

Other methods for counting false positives also exist. Given the complexities and ambiguities surrounding the issue, the reviewers of the South Wales Police LFR trials – the study most analogous to this report – opted for a definition of 'false positives' as, 'a possible match suggested by the [LFR] system that is assessed incorrect by the human operators'. Correspondingly, 'true positives' are defined as, 'a possible match suggested by the [LFR] system that is judged by the human operators'.[236] Rather than taking the 'on the ground' measure of whether a match was confirmed with the actual person on the street, the South Wales criterion of true or false positive locates the role of the *human adjudicators* as central, determining if the computer generated alert is correct or not. Under this definition of false positives, the Metropolitan Police LFR system produced 46 alerts, of which 42 were subjected to an adjudication process. 16 of these were adjudicated by human operators as non-credible. Using the South Wales methodology, this would give a false positive rate, of 38.1% (16/42).

It is beyond the scope of this report to resolve any dispute regarding how false positives are calculated or to provide an accurate agreed upon methodology for measuring the performance of face recognition systems.[237]

However, the research process has yielded insights that may contribute towards this debate, and which are also relevant to consideration of the adjudication process. Significant in this regard is the finding that human judgement of computer-generated matches was extremely unreliable. For example, 26 LFR matches were deemed sufficiently credible to intervene with a person of interest. On only eight occasions did these resolve as a correct identification once an identity check had taken place. This points to the unreliability of human adjudication as a factor that must be taken into account when calculating any false positive rates.

It is also reasonable to assume that an element of error is possible when deciding that a computer-generated match is *not credible*. Some decisions are clear and easy to make (such as inconsistencies in age, gender and race between watchlist and camera images). Other cases are harder to determine. It is therefore impossible to tell with certainty if the computer is correct when an identity was never verified (or

[236] Davies et al. (2019) South Wales police report pp 4-5.
[237] Performance evaluation is an activity conducted by numerous agencies including major US Federal organs including the National Institute of Standards and Technology (NIST), part of the US Department of Commerce.

disconfirmed) in some way (such as through a street-based identity check). This uncertainty applies equally to individuals against whom an intervention was launched but who then became lost in the crowd, and to the 16 individuals considered by operators to be incorrect matches (table 4.3). While it might be reasonable to assume that these were false positives, the absence of an identity check means it cannot be known with any certainty. This points to a further difficulty in verifying claimed accuracy rates in trial scenarios conducted in an operational environment.

For the purposes of this report, conclusions regarding the level of accuracy are solely based on what can be derived with certainty from the collected data. As such, only those matches judged credible following human adjudication can be included. This will necessarily exclude matches generated by the LFR system, but which were not subject to human intervention, or which were not judged credible following human adjudication. In order to reflect this, the terms false positives or true positives are not used. Instead we refer simply to verified correct matches and verified incorrect matches:

- 'Verified incorrect matches' are instances when a computer generated match is judged to be credible by a human operator yet proven incorrect following an identity check.
- 'Verified correct matches' are instances when a computer generated match is judged to be credible by a human operator and proven correct following an identity check.

Across the six test deployments MPS officers engaged with 22 individuals as a direct result of a computer generated match judged to be credible by a human operator.[238] 14 of these (63.64%) were verified incorrect matches, eight were verified correct matches (36.36%). These figures do not take into account the overall number of alerts/matches generated by the LFR system as these are impossible to verify.

4.1.4. Incremental developments across the test deployments

A number of incremental developments occurred as the test deployments progressed. Reflecting the objectives of the deployments as research trials, a 'learning log' was kept and a number of lessons were applied across the period of observation. For example, technical problems hampering the use of handheld mobile devices were addressed ahead of the Romford trials in early 2019. Criteria for enrolment on the watchlist were specified more tightly between the Stratford and Soho test deployments. In other areas, refinements were made to pre-operational

[238] This number does not include individuals who were stopped and/or had their faces scanned as a result of avoiding the live facial recognition cameras discussed separately above.

briefings and relevant governance documentation such as the Data Protection Impact Assessments.

Intelligence units displayed a slightly increased tendency towards adjudicating computer-generated matches as non-credible in later trials, which may suggest increased critical appraisal of LFR technology. Later test deployments also involved additional attention to the location of intervention teams.

The technology itself also improved at several stages. A reportedly more accurate algorithm (NEC's NeoFace M20) was introduced ahead of the 2017 Remembrance Sunday event (before the initiation of research) and apparently more capable cameras were introduced after the Soho test deplo yment in December 2018, and subsequently used at the Romford test deployments in 2019. However, while some lessons were clearly learned during the evaluation period, each deployment generated a number of new and substantive issues. These are discussed below.

4.2. Watchlist Construction

The 'watchlists' were the backbone of the LFR test deployments. The MPS used two separate watchlists/reference databases in each test deployment: an operational list made up of images of persons of interest, and other data about them; and an additional 'blue' list, comprised of images of police officers, technical staff and others involved in trialling the technology, which was used to monitor the system performance.[239]

For the purposes of this report, the term 'watchlist' refers to the MPS operational watchlist of persons of interest. The use of a single target watchlist contrasts with the South Wales Police LFR trials where three separate databases, were used, designated red, amber or green according to the degree of interest the police had and the risk each individual was deemed to pose to public safety.[240]

Once the watchlists were constructed, the LFR test deployment on the ground sought to identify the specific individuals on the watchlist.

Each observed deployment had a bespoke watchlist created for that operation, reflecting local objectives[241] but also, as our research discovered, indicating shifts in criteria for inclusion (both the criteria and the specification of the criteria).

---

[239] See Section 1.2.2 for a discussion of attempts to use the 'blue list' to assess bias in the technology.

[240] Bethan Davies, Martin Innes and Andrew Dawson (2018) *An Evaluation of South Wales Police's Use of Automated Facial Recognition*, Cardiff: Universities' Police Science Institute, Crime and Security Research Institute, Cardiff University.

[241] DPIA July 2018 (emphasis added): *·'To support ongoing policing activity with regards to a specific problem or location*. LFR can provide an *additional* asset to enhance a police response to address a particular issue, such as an increase of a specific crime type within a particular area. This will consist of a bespoke watch-list of wanted individuals or those with conditions not to attend an area based on intelligence and crime analysis.'

4.2.1. The Watchlist Construction Process

The size, focus and composition of watchlists varied across the test deployments. On each occasion watchlist construction involved a complex and laborious task that drew on significant human resources.

In general, watchlists drew information from separate databases. Legacy data handling systems meant relevant data was spread across different databases and each watchlist entry needed to be assembled by manually extracting and merging records from each of these locations. Added to this was the significant scale, complexity and variance of these information systems.

Ensuring accurate and up-to-date information from across these different data sources posed a significant challenge. Such difficulties made compliance with overall standards of good practice complex. For example, the time taken to manually synthesise data from varied databases made it practically impossible to maintain up-to-date records. Rectifying this issue would not only allow a more effective use of police resources and reduced strain on officers, it would also facilitate more robust data management processes.

Partly simplified for clarity of explanation, the main data sources for watchlists can be characterised as:

- The Police National Computer. This holds formal records of encounters of individuals with the police and other criminal justice agencies. For example, it holds data on arrests, charges, court decisions and a range of licensing records (such as driving and firearms).
- The Emerald Warrant Management System (EWMS). This is the MPS system for processing and logging warrants.[242] This logs/includes details of outstanding arrest warrants concerning individuals charged with crimes and wanted for not attending court, skipping bail or non-compliance issues such as breaching court orders, and being wanted for questioning.
- The MPS' own distinct databases for intelligence and offender administration. These include Crime Record Information Systems (CRIS), Criminal Intelligence (CRIMINT) and custody image databases. To manage and merge information from these different databases the Metropolitan Police use a federated platform called 'EAPPs (DP)'.

[242] There is an overlap between the Emerald Warrant Management System and the Police National Computer. This has been best described to the researchers as the Emerald Warrant Management System functioning as a Metropolitan Police Service implementation of the Police National Computer. It therefore adopts similar functions to the Police National computer although there are key differences (such as differences in the rates information is updated) that have an impact on watchlist formulation.

Another source of images used by police *nationally* is the Police National Database.[243] It is of interest to note that many of the images on the Police National Database were already biometrically processed for 'facial searching' long before the LFR test deployments. As stated by the Parliamentary Office for Science and Technology in 2018:

> Since March 2014, police have been able to use images (e.g. CCTV footage) to search against facial images (custody images) on the Police National Database using facial recognition software.[244]

According to the February 2017 Home Office *Review of the Use and Retention of Custody Images*, 'as of July 2016, there were over 19 million custody images on the Police National Database, over 16 million of which had been enrolled in the facial recognition gallery making them searchable using facial recognition software',[245] although 'many of these images are multiple images of the same individual'.[246]

However, in constructing their watchlists the MPS did not in fact make use of this PND database of already processed gallery images or indeed PND custody images at all. Presumably this was because the Metropolitan Police Service ceased populating the Police National Database with its own custody images over five years ago.[247] Rather, they compiled watchlist data from the different sources itemised above. This would also make sense from the position of attempting to use the most up to date images possible.

---

[243] The Police National Database is a distinct and separate entity from the Police National Computer and was established over 30 years later. The Police National Database holds and enables sharing of police intelligence. The Police National Database was introduced based on recommendations stemming from the 2004 Bichard Enquiry review of child protection following the murder of two schoolgirls by Ian Huntley, a school caretaker in Soham, Cambridgeshire. Much of the enquiry focused on the deletion of, and failure to, share information about prior investigations into Huntley for a series of alleged sexual offences that would have prevented his employment at the girls' school. The Police National Database was subsequently established as a means to share intelligence and facilitate better vetting procedures. At the time of writing (April 2019), both the Police National Database and the Police National Computer systems are in the process of being replaced by a new national Law Enforcement Data Service (known colloquially, and more commonly, as LEDS) (see Home Office (2018) *National Law Enforcement Data Programme, Law Enforcement Data Service Privacy Impact Assessment Report*, London: Home Office).

[244] Further: 'the [PND] system calculates a ranked list of potential matches, which are manually inspected to confirm or reject a match. Matches are used for intelligence purposes; the Home Office has said that results are not treated as definitive evidence of identification.' Parliamentary Office of Science and Technology, POSTNOTE 578 June 2018 Biometric Technologies, p. 3. https://researchbriefings.parliament.uk/ResearchBriefing/Summary/POST-PN-0578#fullreport

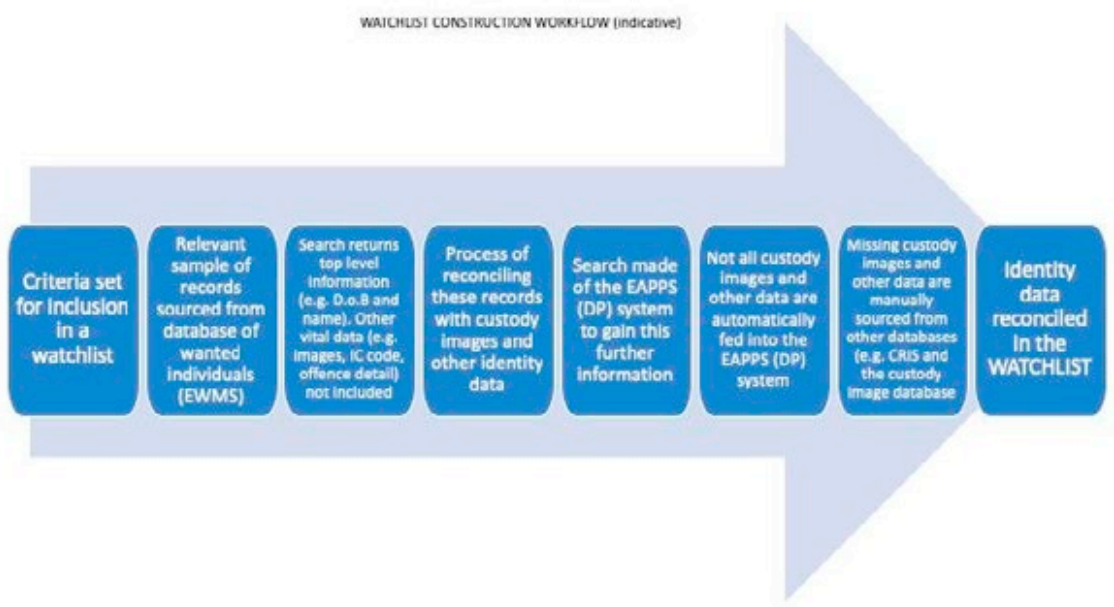
[245] Home Office (2017) *Review of the Use and Retention of Custody Images*, London; HMSO (para 1.5).

[246] Oral evidence to the House of Commons Science and Technology Select Committee (6 Feb 2018 - HC 800) gives the figure of 12.5m images on the PND database searchable using facial recognition software, Baroness Williams of Trafford, Minister of State at the Home Office, clarified that those 12.5 searchable images 'do not equate to 12.5 million people. They equate to 12.5 million searchable images—that is, images that can be used. That is putting it in context. The number of images is more than you think but it does not equate to the number of people'.

[247] According to the February 2017 Home Office *Review of the Use and Retention of Custody Images*, the MPS was one of only nine forces not uploading onto the PND (para 1.5). However, according to the March 2018 Biometric Commissioner's report for 2017, the MPS have now started uploading images of convicted people to the PND: 'I understand that the MPS have now loaded around 60,000 images of convicted people to the PND' p 88, footnote 219. It is important to note that only convicted people are being included. This is presumably responsive to the decision in *R (GC)* v *Commissioner of Police of the Metropolis* [2011] UKSC 21, which held that the retention of images from unconvicted individuals under the Metropolitan Police Service's policy for the retention of custody images was unlawful, although this issue is still under review in respect to police databases generally in Britain.

While the process varied, a simplified and indicative example of how watchlists were constructed by the MPS can be set out as follows. While the explanation of the process is detailed, consideration of these finer grained issues is important when seeking to grasp the significant complexity and burden on officers engaged in this task, and to recognise the challenges of maintaining up-to-date and accurate information.

Fig 4.3. Indicative Workflow for Constructing the Facial Recognition Watchlist



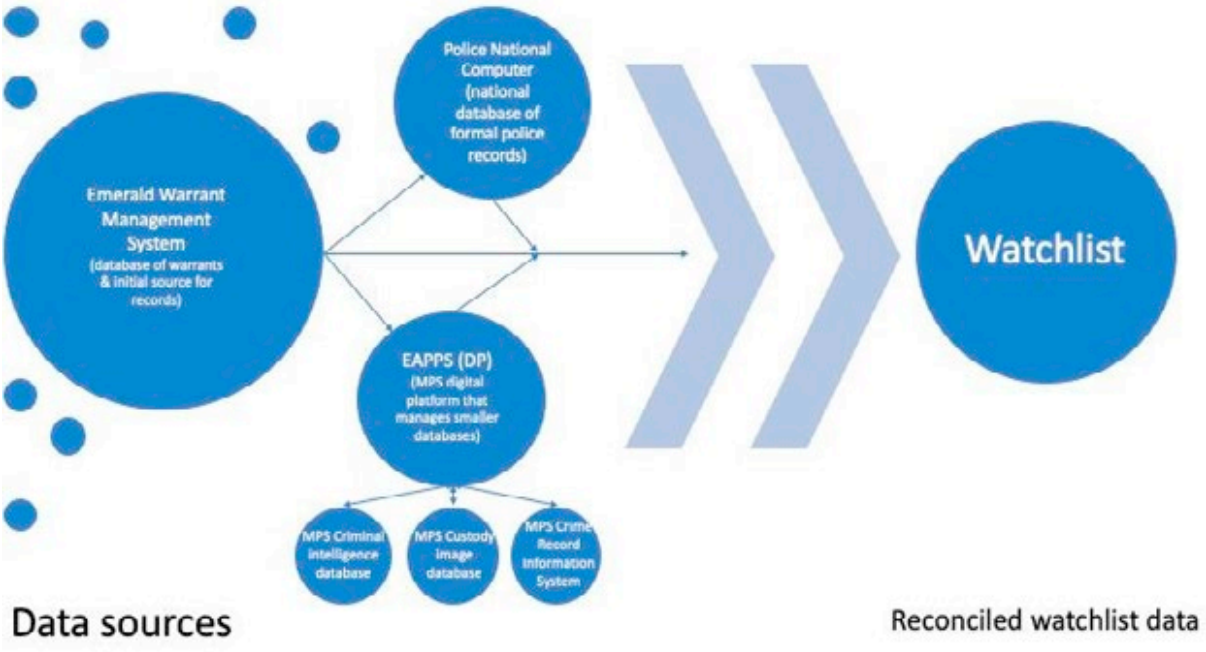
- Records were sourced from the MPS database of 'wanted' individuals, the Emerald Warrant Management System. This allowed individuals who were 'wanted' **for specific offences** to be selected for inclusion in the LFR watchlist. As this is a '*warrant* management system', it can be presumed that 'wanted' here means individuals for whom there are outstanding arrest warrants as offenders.[248] The Emerald Warrant Management System does not hold images.
- When searches are filtered for a specific type of crime (such as 'violent crime'), the Emerald Warrant Management System returns a "front-page" offering limited information, such as the date of birth and name of an individual.
- It was then necessary to retrieve other relevant information from other sources.
- Relevant information that was needed included: custody images, Identity Code (IC) (used to denote ethnicity), offence detail and Police National Computer numbers.

[248] See the discussion of arrest warrants in Section 3.1.2 above.

- Information was then re-keyed into different databases to source this information.
- To achieve this, use was made of the Police National Computer and the MPS' EAPPS (DP) platform.
- A disconnect existed between the EAPPS (DP) platform and the smaller databases it federated and managed. This meant that custody images were not always automatically uploaded from the MPS custody image database to the EAPPS (DP) platform.
- In those circumstances, officers would manually look for and export missing facial images from the smaller MPS custody image database. Officers told researchers that, due to limited interoperability between databases, transferring images from the custody image database involved manually taking screen shots, cropping and then exporting images into the watchlist before reconciling with the text data gained from other sources.
- Biometric processing of watchlist images with facial recognition software.

The use of dispersed data repositories outlined above gave rise to issues regarding (a) the need to manually synthesise information across databases, (c) the currency of records and (d) problems of record duplication.

Fig 4.4. Representation of the Relationship Between Different Data Sources Involved in the Population of Face Recognition Watchlists.[249]



Difficulties encountered in practice with compiling watchlists convoluted this laborious process further still. Some databases systems often held fewer records of individuals than those listed on the Emerald Warrant Management System list of

[249] As explained to the researchers by MPS representatives.

'wanted' individuals. This led to difficulties in sourcing image and other relevant data from elsewhere. Some watchlist entries were incomplete, with some lacking the IC (ethnicity) code of individuals. Databases updated their information at different rates, leading to problems of data currency and the accuracy of whether an individual had been dealt with (and potentially discharged). Records were sometimes duplicated. The highly labour intensive preparatory aspects of the process need to be included in any discussion of the efficiencies of LFR technology.[250] Concerns raised regarding the actual images used to populate watchlists are also referred to in Section 3.3.1.

4.2.2. MPS Data Practice in Relation to Watchlist Criteria

Taking the Emerald Warrant Management System as the starting point for watchlist construction implies that a narrow definition of 'wanted' is being used,[251] meaning that only individuals with outstanding arrest warrants are included on watchlists. It also implies that the conditions attaching to issuing arrest warrants apply, notably that the offence stated in the warrant for arrest must be indictable or punishable with imprisonment.

4.2.3. Variations in Watchlist Criteria and Application

Each observed LFR test deployment had a watchlist created for that specific operation. Whilst the category of 'wanted' (re 'To identify individuals shown as wanted by the police and the courts') was relied on in creating watchlists for all observed test deployments, there were modifications to the threshold for inclusion under this criterion. For example, in relation to the two Stratford test deployments (28 June and 26 July 2018), responses to questions from the researchers over the type and seriousness of the crime were somewhat ambiguous. Violence was almost always stated as reason for an individual's presence on a watchlist. Yet this was regularly supplemented by reference to additional 'other' undefined offences or factors of 'local interest'. Following the second observed trial (Stratford 2), clear attempts were made to address these ambiguities.

From the Soho test deployments (December 2018) onwards, the criteria for 'wanted' became more defined, and was established as 'wanted in relation to violent offences'. This conveyed a sense of commitment to improving specificity as the test deployments progressed.[252] Defining the threshold for inclusion in a more precise

[250] It is likely that this process will become streamlined significantly in the near future. During mid-2018 the Metropolitan Police Service completed its tendering process for providers to create a more integrated data management system (see Government Computing (2018) 'Met Police picks Northgate for MiPS integrated policing deal' available from https://www.governmentcomputing.com/police-bluelight/news/met-police-picks-northgate-mips-integrated-policing-deal). However, claims that this development will overcome the issues highlighted here should be caveated by the facts that this system has yet to be implemented and has never been tested by the Metropolitan Police in relation to face recognition.

[251] See Section 3.3.1.

[252] This section focuses on operational issues. As noted above, significant concerns regarding legal compliance exist. See Section 3.3.

way enables the police to make more effective and justifiable decisions in line with the necessity and proportionality of LFR deployments.[253]

Even within this narrower definition, however, ambiguity remains as to what is meant by 'wanted'.

The data extraction process outlined above – commencing with information on the EWMS system – apparently governed the vast majority of watchlist entries during the trial deployments. This would suggest that only individuals with outstanding arrest warrants were included on any watchlist. However, this was reported to the authors as not always the case in practice, reflecting either the use of criteria other than 'To identify individuals shown as wanted by the police and the courts', or the use of 'wanted by the police' data outside of outstanding arrest warrants. It is important to note that conflicting accounts were given to the researchers regarding other sources of information used to populate watchlists. Officers repeatedly told researchers about other data sources being fed into the compilation of watchlists. At both the second Stratford trial and the final Romford deployment, officers stated that records from the Crime Record Information Systems (CRIS) were entered directly into watchlists.

To understand what is problematic about using the CRIS database, reference should be made to the above discussion in section 3.3.1 about 'wanted on warrant' and 'wanted by the police'. The CRIS database (as indicated by the Humberside definition of 'suspect' above[254]), includes reported and unfiltered victim statements and witness statements as intelligence pertaining to reported criminal incidents. However, it is highly unlikely that CRIS reports as such would pass the more stringent tests for circulation on the Police National Computer. Directly importing MPS CRIS reports into watchlists is therefore a matter of serious concern. It is important to note that this account of the process is contested by others in the MPS. However, the purpose of this research is to report on the information and data presented to us and, therefore, to point out such discrepancies rather than resolve them.

The identification of 'individuals shown as wanted by the police and the courts' was not the only watchlist criterion in use. There were also changes in the invocation and application of the other three criteria identified in the July 2018 Data Protection Impact Assessment. During the first two observed test deployments (Stratford 1 & 2), researchers asked what the basis for inclusion on a watchlist was. Lead operational officers repeatedly responded that 'missing and wanted people' constituted the basis for inclusion. This was reflected in the pre-trial briefings for

[253] However, as noted in the MPS Legal Mandate, the fact that the suspected offence may be serious will not alone render intrusive actions proportionate.
[254] Section 3.3.1.

both test deployments where 'known, missing and wanted' were mentioned. (In terms of the MPS DPIA 23 July 2018 criteria, this falls under (4) 'to assist police in identifying individuals who may be at risk or vulnerable'.)[255] The final four test deployments abandoned any mention of 'missing' as criteria for candidacy on the watchlist. Sound ethical and rights-based reasons may exist for excluding this category. For some, being missing is an active personal choice and they may not consent to being discovered in this manner or at all.[256]

The third criterion listed on the published July 2018 Data Protection Impact Assessment – 'to support ongoing policing activity with regards to a specific problem or location'[257] – was also reported to researchers as playing a role in the creation of watchlists. This is present in the reference to the importance of 'local interest' by a senior officer at one Stratford deployment in response to a question over watchlist construction. Similarly, on at least one occasion, requests were made to add names the watchlist in the minutes preceding deployment based on the introduction of local intelligence brought by officers at the pre-trial briefing.

4.2.4. Data Currency

National (i.e. Police National Computer) and local (MPS) databases operated on different time frames. National databases were updated more regularly than local iterations. This, combined with the time consuming task of manually re-keying information across multiple databases, meant that watchlists were always out of date to a certain degree by the time of deployment. For instance, for the Soho test deployments the watchlist was constructed nearly two weeks before deployments. Others were updated closer to the time of the test deployment.

Issues to do with the accuracy of the watchlist played out on several occasions, when individuals were stopped on the basis of outdated information. For example, an incident involving one matched individual during the first Soho trial highlighted disparities in the currency of information across databases. The LFR system matched an individual with a person listed on the Metropolitan Police Emerald Warrant Management System as wanted for serious violent offences. When stopped by officers the matched individual claimed his serious offence had been dealt with by the criminal justice system. Following further investigation, the person's entry on the more recently updated Police National Computer revealed that they were wanted in relation to malicious communications (a lesser offence).[258] Whilst undoubtedly a

[255] For a discussion of the impact of these categories on the necessity test, see Section 3.

[256] It is important, however, to report potential differences between vernacular and policing uses of the term 'missing'. Members of specialist MPS units interviewed for this report stated how, for them, the 'vast majority' of wanted cases they were concerned with involved people suspected of being involved in serious criminal activity. A large proportion of those were stated to be minors.

[257] This connects with the discussion on matching deployments to purpose below, see section 4.3.

[258] This is alert number two, first Soho test deployment, 17th December 2018 (Table 4.7.).

serious offence with real consequences for victims, it is unlikely this more recent offence would have been sufficiently serious to be included in the initial watchlist.[259]

Outdated information can also complicate the measuring of system effectiveness. At one of the Romford test deployments a 15 year old male was matched to the watchlist as he walked past the cameras.[260] A decision was made to intervene and the individual was questioned. This was a verified correct match but he had already been dealt with by the criminal justice system in the time between watchlist compilation and the LFR test deployment, and so should not have been included on the watchlist under the stated criteria for enrolment. This individual also generated an alert a second time later in the afternoon as he passed the cameras again.

This raises a number of issues. In the first instance, they raise the possibility of listed individuals who have already been dealt with by the criminal justice system being inappropriately subject to interference by the LFR system. This becomes an additional concern when LFR is deployed on a necessity calculation intended to address serious crime but also comes to include more minor offences.

Two elements of the Surveillance Camera Code of Practice are relevant here:

> Any information used to support a surveillance camera system which matches against a reference database for matching purposes should be accurate and kept up to date.[261]
>
> Any use of technologies such as ANPR or facial recognition systems which may rely on the accuracy of information generated elsewhere such as databases provided by others should not be introduced without regular assessment to ensure the underlying data is fit for purpose.[262]

The time-consuming process of populating watchlists also creates challenges for the internal compliance mechanisms governing the use of LFR. As discussed earlier, police and other agencies are required to complete a Data Protection Impact Assessment (DPIA) under the Data Protection Act 2018. The purpose of creating a DPIA is to assess the potential impact of the data processing involved, its lawfulness and ways of mitigating harms and to specify internal mechanisms to ensure compliance with the law.

---

[259] Interestingly, when the arresting officer later visited the van to check the LFR footage he made an instant judgement that this was a false positive. Had he possessed a mobile device a stop would have been less likely.

[260] Alert number five, first Romford test deployment, 31st January 2019 (Table 4.9.).

[261] 'Surveillance Camera Code of Practice Pursuant to Section 20 of the Protection of Freedoms Act 2012', Home Office, para. 2.6. The watchlist constitutes the reference database for LFR systems.

[262] 'Surveillance Camera Code of Practice Pursuant to Section 20 of the Protection of Freedoms Act 2012', Home Office, para. 4.12.1. Evidently the watchlist itself relies on 'information generated elsewhere'.

In accordance with recommendations of the London Police Ethics Panel Interim Report on Live Facial Recognition (2018), the MPS published the 23 July 2018 DPIA on their dedicated LFR website. There was no legal requirement for the Metropolitan Police to publish this. As stated by the Information Commissioner's Office:

> S64 [of the Data Protection Act 2018] sets out requirements for controllers with regard to DPIAs. It is considered good practice for these to be updated regularly. Controllers can publish them, but this is not a requirement.[263]

This online publication of LFR Data Protection Impact Assessments is thus regarded by the researchers as an attempt by the MPS to act in good faith and pursue best practice.

The Data Protection Impact Assessment published online remains in place at the time of writing (April 2019). It is dated 25th July 2018 and was developed in advance of the second Stratford trial. The MPS Legal Mandate describes the DPIA (formulated in compliance with the new Data Protection Act 2018) as a 'living document' that 'is reviewed before every deployment'.[264]

On the issue of data accuracy, the 23 July 2018 Data Protection Impact Assessment states that watchlists are created in advance of deployments but are 'reviewed again no more than 2 days prior to the operation to ensure that it only contains relevant and actionable data'. This statement was retained in the next iteration of the Data Protection Impact Assessment (covering the Soho test deployments) but removed ahead of the 2019 Romford deployments. As a result, the Data Protection Impact Assessment covering the example from Soho above, and the public facing 23 July 2018 DPIA – together covering both Stratford and Soho test deployments – created an internal safeguard that pledged a review of watchlist data within two days of deployment. The difficulties of assembling large watchlists and way this issue played out in the incidents highlighted above severely restrict the likelihood that this commitment could be upheld.

4.3.Matching Deployment to Purpose

Any evaluation of the efficacy and efficiency of LFR test deployments must naturally consider how well the actual deployment related to the stated overall objectives and specific purposes for that deployment. This is also relevant to the necessity calculation required by human rights law.[265] In a number of test deployments, one of

[263] Written submission to this report by the Information Commissioner's Office.
[264] MPS Legal Mandate 23 July 2018, p.7.
[265] See Section 3.

the purposes of using LFR technology related to the third category identified in the MPS DPIA 25 July 2018:

> To support ongoing policing activity with regards to a specific problem or location: LFR can provide an additional asset to enhance a police response to address a particular issue, such as an increase of a specific crime type within a particular area. This will consist of a bespoke watch-list of wanted individuals or those with conditions not to attend an area based on intelligence and crime analysis.[266]

The observation period took place against a backdrop of an escalating incidence, and associated growing public concern, over serious violent crime in the capital. Worsening knife crime in particular has become a legitimate focus of this concern. Home Office statistics reveal that 2017-18 saw 285 knife-related homicides, the highest figure since 1946, with the highest concentrations per capita by a significant margin occurring in London.[267] In early 2019 chairperson of the National Police Chiefs Council Sara Thornton labelled the rise 'a national emergency', Mayor of London Sadiq Khan funded a new Violent Crime Taskforce and Home Secretary Sajid Javid requested additional resources from the Treasury to tackle the issue. In this context, it is important to recognise that LFR deployments directly led to arrests of individuals wanted in relation to possessing weapons. However, as recognised by the MPS: '[t]he fact that the suspected offence may be serious will not alone render intrusive actions proportionate.' [268]

Police uses of surveillance measures typically satisfy the legitimate aim test on the basis of protecting the public from serious crime and upholding public order,[269] and this context of violent crime reinforces arguments concerning the legitimate aim pursued by LFR. However, the necessity of such measures in a democratic society must still be satisfied. This requires an examination of both potential utility[270] and potential human rights-related harm to generate an overall evaluation of whether the measures is necessary in a democratic society.

One key element when evaluating issues of necessity and, by extension, proportionality is a consideration of the stated purpose of LFR test deployments and, crucially, analysis of the extent to which the use of the technology is 'rationally connected' to this purpose.[271] This issue may be addressed by comparing the

[266] MPS DPIA July 2018, p.2.
[267] Danny Shaw, 'Ten charts on the rise of knife crime in England and Wales', *BBC News*, 14 March 2019. Available at: https://www.bbc.co.uk/news/uk-42749089.
[268] MPS Legal Mandate 23 July 2018, p.5.
[269] See, for example, ECtHR, *Weber and Saravia v. Germany*, App no 54934/00, 29 June 2006, paras. 103-104; see also *R (on the application of Roberts) (Appellant)* v *Commissioner of Police of the Metropolis and another (Respondents)* [2015] UKSC 79 para 3.
[270] i.e. how 'useful' LFR techniques are, in light of the legitimate aims and specific purposes pursued.
[271] Whether the measure is 'rationally connected to the objective' is particularly emphasized in the consideration of proportionality frequently employed by the English courts in respect to issues of privacy/ECHR Article 8. Lord Reed in *Bank*

rationale for LFR use offered in intelligence briefings and its application to address this defined purpose. An intention to tackle violent crime was a stated feature of all LFR intelligence briefings observed by the researchers. For the second trial in the Stratford Ward,[272] violent crime – broken down by police into 'knife crime', 'violence' and 'robbery' – was stated as a headline justification for the LFR test deployments.

Analysis of the rationales given for LFR deployment also generate wider considerations with regard to its alignment to the stated objectives and overall purpose. Questions over whether LFR is appropriately directed to a specific threat involve considering at least two dimensions: are cameras patrolling the spaces identified as being at risk and are cameras patrolling the spaces identified as being at risk at the appropriate time. It is also worth emphasising that a purely instrumental calculation of efficacy and efficiency would likely involve the same considerations.

4.3.1. The Alignment of Deployments to the Stated Objectives and Overall Purpose.

Most ethical guidance, and legal and oversight provisions governing surveillance require a clearly prescribed application. This is to prevent surveillance measures inappropriately 'creeping'[273] into other activities. It is therefore important to align the use of LFR with a specific purpose. Any shift in purpose threatens legitimacy.[274] Two elements are relevant in this regard: the type of offence and the way in which the offence is addressed.

Type of offence.

Additions to the watchlist based on reasons other than those originally specified is perhaps the most obvious way that an identified purpose may shift. This possibility was articulated to the researchers by one senior officer during the second Stratford trial deployment who mentioned that the primary reason for individuals being placed on the watchlist was for being wanted in connection with violent offences, before stating that other 'locally relevant' offences also constituted a basis for inclusion.

Other processes may also dilute the stated purpose of this measure. As noted below, the test deployments demonstrated how it is possible for individuals stopped on the basis of a verified incorrect LFR match to be then arrested for another reason (e.g. alert one, Table 4.7.). While this may suggest that LFR has a wider role in apprehending offenders, three caveats exist. These are: compliance with the necessity calculation underpinning the deployment, a potential broadening of police

Mellat v *HM Treasury (No 2)* [2013] UKSC 39, [2014] AC 700, para 74.

[272] Stratford is one of 19 policing wards in the London Borough of Newham.

[273] See generally Marx, G. (1989) *Undercover: Police surveillance in America*, Oakland, CA: University of California Press.

powers, and questions over whether the presence of LFR creates the circumstances in which an offence is then committed. These points are developed below in sections 4.4. and 4.9.

Manner of addressing the offence.

This relates less to *what* is being addressed but rather to *how* it is addressed. In the first test deployments observed (Stratford), LFR use was regularly justified in briefings on the basis of several perceived benefits. The detection of wanted individuals was always stated as the central purpose yet supplementing this were additional claims of ancillary benefits including: the disruption of crime, crime displacement and deterrence effects. Using LFR for detection, deterrence, intentional crime displacement or disruption involves clear differences in the purpose, affecting necessity calculations. For example, a wide range of inexpensive and non-intrusive/non-biometric policing options, such as the placement of visible uniformed officers, exist to deter potential offenders form a particular space at a specific time.[275]

A related issue concerns how claims for effectiveness are evidenced. A key part of the technical evaluation of these test deployments focuses on the technological performance of LFR systems. However, the same standard of analysis is not brought to other areas of claimed effectiveness. For example, deterrence effects, even when apparent,[276] are often difficult to substantiate.[277] Yet no evidence was offered to support these claims of effectiveness in these wider roles.

LFR was also justified on the basis of offering reassurance to the community by providing a visible symbol that crime was being tackled. Issues of community engagement and legitimacy are discussed above in section 3.4.2. During the Stratford test deployments the visible presence of LFR was claimed to have a positive effect in allaying the fear of crime. One of the difficulties with making such claims is the challenge of substantiating them. Accurate measurement of public fear of crime is notoriously complex and has long constituted a subject of heated criminological

[275] This form of deterrence is well established in criminological scholarship. It is often articulated through the argument that crimes are more likely to occur when three elements combine: a motivated offender, an opportunity, and the absence of 'capable guardianship' (i.e. the presence of some form of authority) (e.g. see Bottoms, A. E., and Wiles, P. (2002) 'Environmental Criminology' in Maguire, M., *et al* Eds. *The Oxford Handbook of Criminology*. Oxford: Oxford University Press).

[276] While it is impossible to draw robust conclusions from the activities occurring on a single day, officers with an intimate knowledge of policing the area expressed credible, if anecdotal, claims that the deployment of live facial recognition had a deterrent effect at one of the Stratford trials.

[277] An extensive academic literature has focused on the deterrence effects security measures more generally (Akers, R. (1990) "Rational choice, deterrence, and social learning theory in criminology: The path not taken," in *Journal of Criminal Law and Criminology*, 81, 653-676; Hayward, K. (2007) "Situational Crime Prevention and its Discontents: Rational Choice Theory versus the 'Culture of Now," *Social Policy & Administration* 41, no. 3: 232 250; Farrell, G. (2010) 'Situational Crime Prevention and Its Discontents: Rational Choice and Harm Reduction versus "Cultural Criminology"', *Social Policy & Administration*, vol. 44, no. 1: 40–66), and of surveillance camera devices more specifically (e.g. Tilley, N. (1998) 'Evaluating the Effectiveness of CCTV Schemes', in C. Norris, J. Moran and G. Armstrong (eds.) (1998) *Surveillance, Closed Circuit Television and Social Control*, Aldershot: Ashgate, pp. 139-175; Fussey P (2008) Beyond Liberty, Beyond Security: The Politics of Public Surveillance. *British Politics* 3(1): 120–135). This field is characterised by significant debate. Reservations over deterrence claims include the difficulty of measuring 'non-events' (i.e. an absence of crime) and methodological concerns over the amount of time needed to observe a genuine deterrence effect.

debate.[278] When accounting for these complexities as a whole, it is extremely difficult to claim widespread public benefit and support without a high standard of evidence.

Extending the purpose of LFR deployment to cover these wider ambitions of deterrence and public reassurance raises an additional question: to what extent do various justifications cohere and support each other? The MPS placed considerable importance on public engagement during the observed test deployments. While there is debate over the success and articulation of this approach,[279] this ambition was prominent during all planning meetings and was continually articulated throughout the test deployments. However, officers in intervention teams repeatedly expressed frustration that this public engagement – including online publicity, leafleting and other forms of visible police-public encounters – while seen as important for issues of public confidence, at the same time undermined the detection function of the technology. This was directly blamed for the very low level of matches during the second Stratford trial by some officers, with one stating that 'by the afternoon everyone in the neighbourhood knew about the trial. Information had gone out on local networks and social media'.

4.3.2. Matching Deployments to Spatial Intelligence: Are cameras patrolling the spaces identified as being at risk?

To satisfy the necessity test and to conform to provisions in the Surveillance Camera Code of Practice regarding specificity of purpose,[280] cameras need to be sited in an

[278] There is a long history of examining the fear of crime in criminological scholarship, and it constituted a principal area of concern throughout the 1980s and 1990s. Despite its longevity, only limited agreement has emerged from this debate. Whilst it is generally accepted that levels of fear and objective measures of crime are not closely related, critical scholarship has pointed to: the under-representation of key social groups in measurements of crime fearfulness (Skogan, W.G. (1990) *Disorder and Decline: crime and the spiral of decay in American neighbourhoods*, New York: Free Press); difficulties of quantifying highly emotive feelings and a tendency towards measure an artificial 'amount' of fear rather than its implications (Pain, R., Williams, S. and Hudson, B. (2000) *Auditing Fear of Crime on North Tyneside: A Qualitative Approach,* British Criminology Conference Selected Proceedings Volume 3); the tendency to categorise 'others' as 'criminal' (Hale, C. (1996) 'Fear of crime, a review of the literature', International Review of Victimology 4: 79–150), particularly those already subjected to police measures (Coleman, R., and Sim, J. (1998) 'From the Dockyards to the Disney Store: Surveillance, Risk and Security in Liverpool City Centre', in *International Review of Law, Computers and Technology*, 12(1) pp. 27-45); and the tendency of individuals to coalesce a deeper range of social anxieties as an expression of fear (Young, J (1987) 'The Tasks Facing a Realist Criminology', in *Contemporary Crises,* 11. pp. 337-356). Debate also exists over whether security measures, particularly visible surveillance cameras, reduce or exacerbate public fears. One of the earliest published evaluations of surveillance camera performance, for example, was an examination of CCTV and fear of crime in New York City (Musheno, M., Lavine, J., and Palumbo, D. (1978) 'Television Surveillance and Crime Prevention: evaluation of an attempt to create defensible space in public housing', in *Social Science Quarterly*, 58(4) pp. 647-656). This study concluded that no positive impact on fear could be identified. Other studies have pointed to more complex effects, such as the tendency to enhance feelings of safety among those that already feel secure, while exerting less impact on those who avoid particular spaces owing to fear (Gill, M. and Spriggs, A. (2005) 'Assessing the impact of CCTV', Home Office Research Study no. 292. Home Office: London). Part of this complexity lies in the fact that different sections of society experience fears of crime and respond to policing interventions differently, and at different times. These debates highlight the level of disagreement in the field and the difficulties in making substantive claims on behalf of any social group.

[279] See Section 3.4.2.

[280] The first principle of the Surveillance Camera Code states: '1. Use of a surveillance camera system must always be for a specified purpose which is in pursuit of a legitimate aim and necessary to meet an identified pressing need.' This is amplified further in the new code on The Police Use of Automated Facial Recognition Technology with Surveillance Camera Systems: Section 33 Protection of Freedoms Act 2012 (March 2019: 'In essence there must be clarity as to the problem which is to be addressed by the use of AFR and which can be evidenced, and the purpose to which AFR is to be operated. Such purposes may include matters such as the prevention and detection of crime, public safety, national security etc. There should be clarity

area where specific risks have been identified.[281] For the observed test deployments, decisions as to where to locate the cameras took into account specific identified risks, based on a local intelligence picture and developed by drawing on a range of further information, including the prevalence of particular offences and experiences of local police.

Decisions over the location of cameras were additionally influenced by technical and operational considerations such as the ability to situate a surveillance van in a particular place, the cameras' field of view, possibilities for locating intervention teams, risks to the public, risks to the police, and so on. Thus, it is reasonable to expect some margin of discretion regarding the exact location of cameras, based on operational realities. Taking such contingencies into account, it is still possible to assess the ability of the deployment to respond effectively to the identified threat/risk.

The second Stratford test deployment sought to use LFR to complement a Newham-wide initiative targeting violence in the borough. Further justifications drew on a range of borough-level statistics and Newham's unfavourable position (in terms of crime) in relation to other parts of the London metropolitan area. These included statistics showing that, at the time of the test deployment, of 32 London boroughs Newham had the fourth highest rate of violence, the fifth highest rate of robbery and the tenth highest rates of knife crime.

The LFR test deployment took place in Westfield Shopping Centre. However, the local intelligence picture identified high concentrations of offences in a location some distance away from Westfield Shopping Centre, and the other side of several train lines, a large carriage way and another shopping centre. High concentrations of offences also existed in another part of Stratford regarded by local officers who had a detailed knowledge of the area as entirely distinct from the Westfield shopping mall.[282] In addition, senior officers stated that a significant proportion of criminality in question was "driven by homeless people" in this particular area. Regardless of the veracity or otherwise of this claim, there are very few homeless people at Westfield shopping centre, the site of this LFR deployment, it being a largely private space and subject to stringent place management administration.

Therefore, for this test deployment, intelligence and statistics were taken from surrounding areas and not the site of the test deployment itself. Members of local police units also re-confirmed this point to the researchers at the end of the trial.

---

provided as to why it is considered necessary to use the intrusive capabilities of AFR in such circumstances rather than simply desirable. The availability of AFR capability to address a particular issue is not in itself justification for its use on the grounds of necessity. Just because you can doesn't mean you should. A record should be made as to the case of necessity' (para 9.6).

[281] This is, of course, only one element of the necessity test.

[282]This point was further expressed to researchers by local officers engaged in the test deployment.

4.3.3. Matching Deployments to Temporal Intelligence: Are cameras patrolling the spaces identified as being at risk at the appropriate time?

The last four test deployments involved cameras being sited more closely to areas identified by local intelligence as experiencing problems. In addition, operations were focused more clearly on specific (serious) types of offences.

However, assessing the ability of a LFR deployment to meet the stated objectives involves consideration of a time component. In Soho, pre-deployment briefings provided detailed explanations of where these more serious violent offences were clustered. Due to their association with the area's night time economy, many of these activities intensified at weekends and between the hours of 23:00 and 04:00. The LFR test deployments took place on a Monday and Tuesday roughly between the hours of 08:00 and 16:00.

A similar dynamic figured in the Romford test deployments. Several important tactical, operational and technological reasons informed the decision to operate at times different from that suggested by the intelligence picture. These included the technical evaluation need to establish technological capabilities in daytime, the availability of officers, operational priorities and the undesirability of redeploying stretched night time teams on a weekend before Christmas. However, this temporal disconnect again points to tensions pointed to above between conducting a trial as a 'research' enterprise and conducting an active operation.[283] A trial requires a sense of testing to understand capability (e.g. camera and recognition performance in low light), whereas a deployment needs to evidence the necessity of this particular intervention including its ability to address the identified aim (e.g. tackling crime in the night-time economy).

4.4. Consent

The role of public consent constituted a contentious debate surrounding the LFR test deployments. Like CCTV, LFR is classified by the MPS as a form of overt surveillance and the consent of affected individuals is seen as fundamental. The Surveillance Camera Code of Practice states:

> The government considers that wherever overt surveillance in public places is in pursuit of a legitimate aim and meets a pressing need, any such surveillance should be characterised as surveillance by consent, *and such consent on the part of the community must be informed consent and not assumed by a system operator.* Surveillance by consent should be regarded as analogous to policing by consent. In the British model of policing,

[283] See Section 3.1.

> police officers are citizens in uniform. They exercise their powers to police their fellow citizens with the implicit consent of their fellow citizens. Policing by consent is the phrase used to describe this. It denotes that the legitimacy of policing in the eyes of the public is based upon a general consensus of support that follows from transparency about their powers, demonstrating integrity in exercising those powers and their accountability for doing so.[284]

Measures undertaken by the MPS that bear on consent overlapped with attempts to promote public reassurance and to test public opinion.[285]

For consent to be meaningful, several conditions are important:(1) any consent needs to be informed; (2) clear alternatives must exist in order for people to exercise a different choice; and (3) alternative choices much be exercised without fear of penalty. All of these elements are relevant to the deployment of LFR. Common to other aspects of the LFR test deployments, the practical application of this technology generates a range of varied and complex issues.

4.4.1. Informed Consent

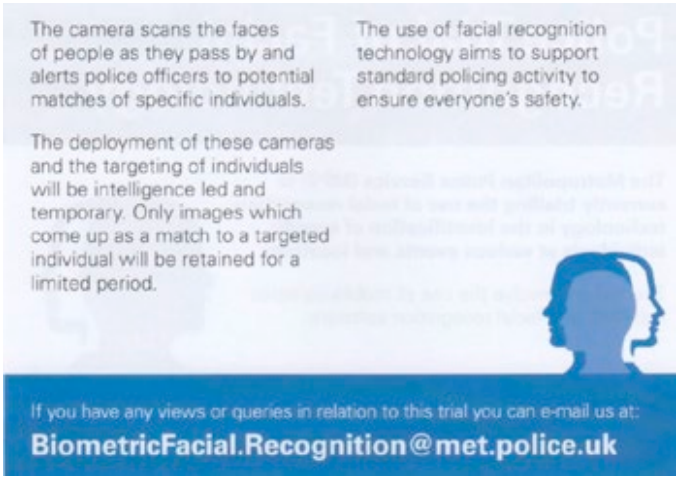
In line with the Surveillance Camera Code requirement quoted above – 'consent [to overt surveillance] on the part of the community must be informed consent and not assumed by a system operator' – the MPS pursued a number of strategies intended to ensure that public consent for LFR constituted *informed* consent. Uniformed officers were stationed at all test deployments, briefed to explain the role of the technology, deployments, and to direct members of the public to further information (such as the public LFR website). The researcher regularly witnessed uniformed officers explaining the purpose of the test deployments at great length to members of the public and, on more than one occasion, acting with patience and professionalism to de-escalate confrontations.

Uniformed officers were also issued with leaflets providing written information about the test deployments. These were issued at all test deployments observed. 1,400 leaflets were printed in advance of the second Stratford trial. There has been some debate over the degree to which these leaflets were distributed to the public. Some civil society groups have stated that very few leaflets were given out at test deployments they observed. Researchers witnessed uniformed officers distributing this information on a regular basis. Pre-trial briefings also placed significant emphasis, and provided clear instructions on, the importance of leafleting.

[284] S1.5 p3. Emphasis added.
[285] Wider issues of public engagement are discussed above in Section 3.4.

Plate 4.1. Metropolitan Police Service LFR Public Information Leaflet (Stratford test deployments, 2018, front)

Plate 4.2. Metropolitan Police Service LFR Public Information Leaflet (Stratford test deployments, 2018, back)

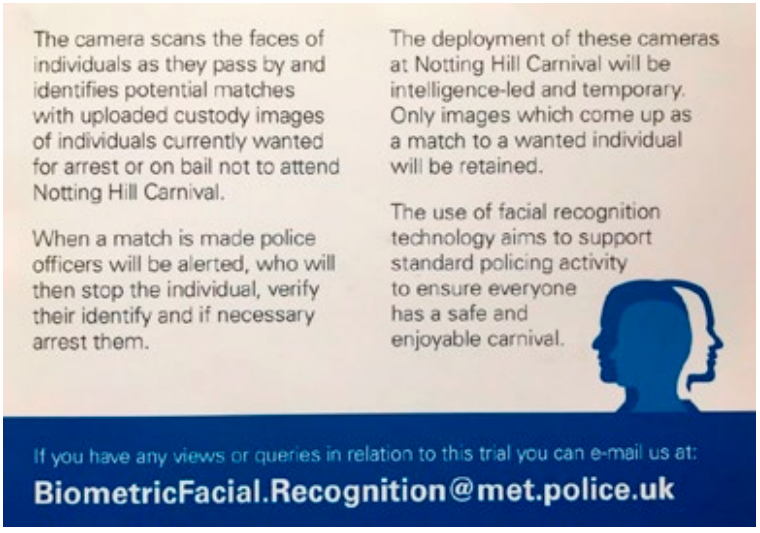


Important here is to delineate issues of public communications from those of consent. In doing so, a key question emerges over the degree to which consent can be considered informed on the basis of the information supplied by the MPS. For example, the information provided transparency regarding the time and location of the LFR test deployments yet there was less clarity over the purpose of the deployment, who was likely to be the subject of surveillance, and how additional information could be ascertained. For instance, improvements in communication strategy could include directing people to more detailed information by including a QR code, website address or other means of accessing online content. An email address for queries was provided on the leaflets but when researchers asked about the volume of emails received, they were informed that this facility was rarely used by the public.

Of additional note here is that leaflets for the Stratford test deployments (June and July 2018) contained less information on the purpose and likely subjects of surveillance than those provided at the earlier 2017 test deployment at the Notting Hill Carnival (see **Plates 4.3. & 4.4.).**

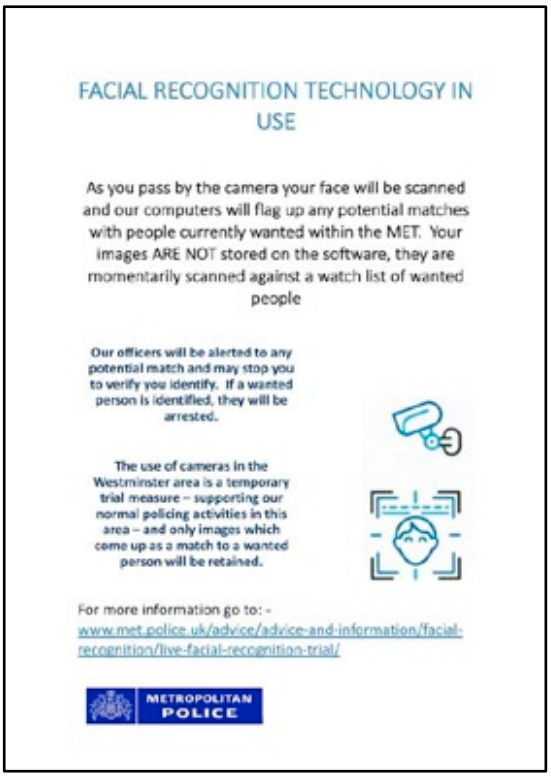
Plate 4.3. Metropolitan Police Service LFR Public Information Leaflet (Notting Hill Carnival test deployment, 2017, front)

Plate 4.4. Metropolitan Police Service LFR Public Information Leaflet (Notting Hill Carnival test deployment, 2017, back)



Some of the more detailed information was again included in updated leaflets used for the two Soho test deployments (**Plate 4.5**.). However, the less detailed Stratford leaflets were again used for the later Romford test deployments

Plate 4.5. Metropolitan Police Service LFR Public Information Leaflet (Soho test deployments, front)



Signage was also an important part of MPS efforts to obtain informed consent (see immediately below). Signs were used as a means to inform the public they were entering an area of camera coverage. There has been some public disagreement regarding the placing of these signs. Our independent photographs from each observed trial are included below. From the perspective of camera operators inside the van, people positioned next to signs were out of frame on each observed trial except for the morning of the first Soho trial (see **Plate.4.7.).** This meant that, with the exception of the first Soho trial, an individual reading or standing next to a sign was out of LFR camera range for each LFR deployment.

Plate 4.6. Positioning of Information Boards in Relation to LFR van at Stratford Test Deployments (board and cameras in same location for both deployments 28/6/2018 and 26/7/2018)

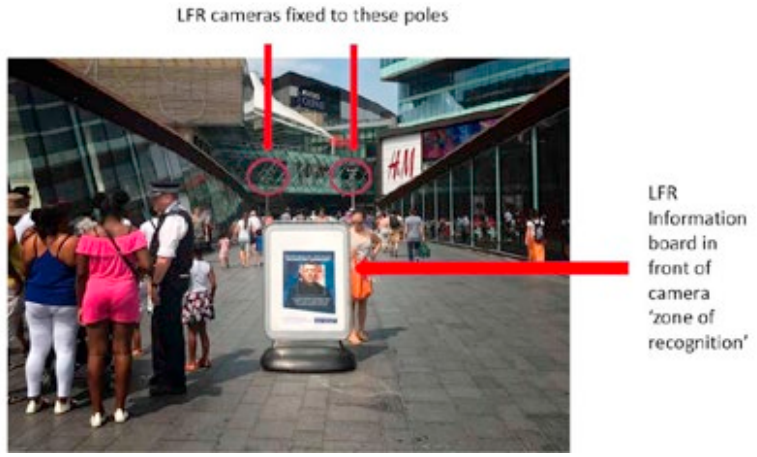


Plate 4.7. Positioning of Information Boards in Relation to LFR van, First Soho Test Deployment (morning deployment at Cambridge Circus 17/12/2018)

Plate 4.8. Positioning of Information Boards in Relation to LFR van, First Soho Test Deployment (afternoon deployment at Leicester Square 17/12/2018)

Plate 4.9. Positioning of Second Information Board next to LFR van, Second Soho Test Deployment (additional to information boards placed outside the zone of recognition) (Leicester Square 18/12/2018)

Plate 4.10. Markings on LFR van, First Romford Test Deployment (31/01/2019)

Plate 4.11. Positioning of Information Boards in Relation to LFR van, First Romford Test Deployment (31/01/2019)

Plate 4.12. Positioning of Information Boards in Relation to LFR van, Second Romford Test Deployment (14/02/2019)*

*Sign placed around two metres further away from the LFR van than at the previous test deployment.

For the first Soho trial [17 December 2018] the LFR van was stationed in Cambridge Circus, at a busy intersection between Shaftesbury Avenue and Charing Cross Road. As visible in **Plate 4.7.**, individuals would have already passed through the camera's field of view before being alerted to their presence by the signs. The LFR van used as a control room was also unmarked, preventing easy identification. Both of these issues were rectified to some degree when the van relocated to Leicester Square for the afternoon where an LFR sign was placed against the van, (see **Plate 4.9.**). However, there was no opportunity for an individual to exercise informed consent during the morning deployment.

Information boards were positioned further away from and outside of the cameras' field of view for each of the other test deployments. Questions exist over the degree to which this provided the detail and time needed for reflection in order to offer meaningful consent. Some signs placed close to the ground, as in both Soho trials, may be unnoticed as people pass by. This point was expressed by Liberty during their interview for this report: 'very small signs that people can't read isn't informing the public'.[286] Moreover, the high degree of visual and audible distractions experienced by pedestrians in some locations, such as Leicester Square (see **Plate 4.8.**), may further reduce the prominence of LFR signage. In all cases, an individual would have entered the cameras'[287] field of view within a few seconds of encountering an information board.

Other civil society organisations have also challenged the extent to which consent is informed or meaningful. Director of Big Brother Watch, Silkie Carlo, focused especially on the data processing and biometric processing aspects:

> No, there's no consent. No, there's no information, so people aren't informed. They're not in any meaningful sense of the word, even the vernacular word or the legal meaning of the word, there's no meaningful consent process whatsoever. You certainly can't withdraw consent. It has real life significance and legal impacts as well, serious risks to individuals involved. Data collection that people aren't informed about. And biometric data processing. … We've [probably spoken to] more people than anyone, members of the public, than any other group because we've been at every deployment except the first one in Stratford, we've been at every deployment since the announcement of the trial, when we were in Notting Hill Carnival, the second one, and then Stratford, Romford, Leicester Square, all the rest of it, and we've been there beginning to end handing out leaflets, talking to people. I would

[286] Interview with Hannah Couchman, Advocacy and Policy Officer, Liberty.

[287] All observed test deployments used two cameras. For 'static' deployments, such as Stratford, they were situated in close proximity to each other (see **Plate 4.6.**). For mobile deployments (Soho and Romford), they were located on top of the same van (see **Plate 4.9.)**. The two cameras worked in tandem, serving to each supplement and widen the other's field of view.

> struggle to recall anyone who said to me, 'Oh, yes, I know about this.' The people see the sign and go, 'That's good,' or 'That's bad,' but in a responsive way and … I could count on one hand the amount of people we've spoken to that seemed to be really informed about what it actually is.[288]

A key conclusion that can be drawn here is the importance of maintaining a clear distinction between the purposes of providing publicly available information. What might be appropriate in respect to issues of public support is not necessarily sufficient or well targeted enough to support individual consent. During test deployments individuals were required to make an informed decision in a very short time-frame, a factor exacerbated by the limits on prior knowledge amongst the public.

4.4.2. Consent and opportunities to exercise a different choice

Another element of consent concerns the availability of alternative choices. Even assuming that signs were prominent, were duly noted by pedestrians, and were positioned to allow time for proper consideration, consent could only be called meaningful if an opportunity existed to make an alternative choice. There are several issues at play here.

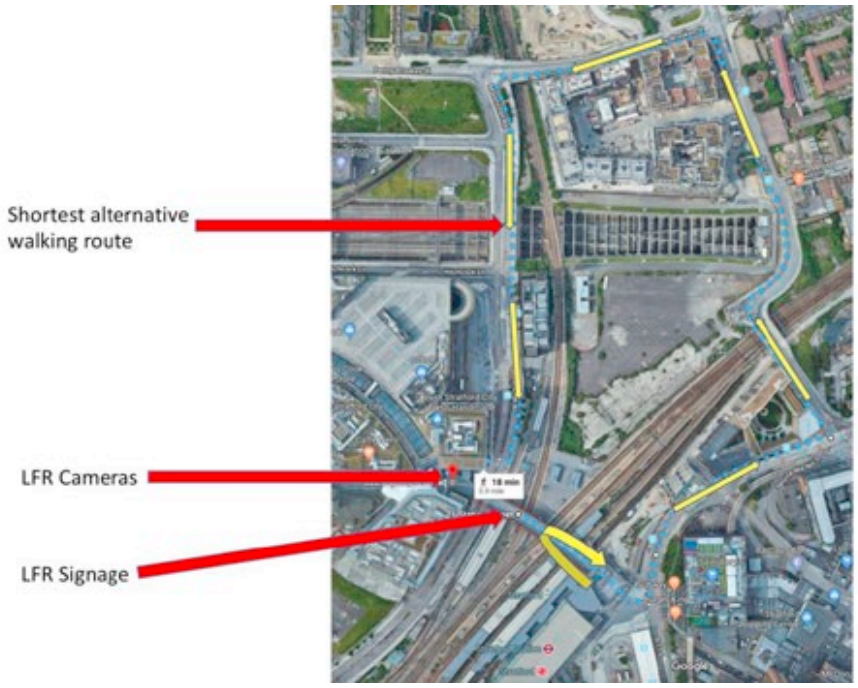
In the first instance, it is difficult for an individual to gain an accurate assessment of a camera's coverage and their position in relation to it. There are no indications of this in any information disseminated to the public, and an assessment would be difficult to make on the available visual cues (e.g. signage and the appearance of cameras). Added to this, studies have shown a tendency for over-estimating the capability of police technologies.[289] As such, the technological limitations of LFR and the ease with which the cameras could have been avoided at some test deployments may not have been clear to the public.

Opportunities for pedestrians to bypass the cameras' field of view and continue walking towards the same destination varied across the test deployments. Crossing the street would have been sufficient to avoid the camera's gaze in Romford, for example. In Soho, other entrances to Leicester Square exist. In Stratford, however, avoiding the cameras would have required either a walking detour of an additional 18 minutes or paying to pass through the Underground Station ticket barriers to reach the same point (see **Fig 4.5.**).

[288] Interview with Silkie Carlo, Director, Big Brother Watch.

[289] e.g. Gates, K (2013). "The Cultural Labor of Surveillance: Video Forensics, Computational Objectivity, and the Production of Visual Evidence." *Social Semiotics*. 23:2 (2013): 242-260.

Fig 4.5. Shortest Alternative Walking Route Avoiding Stratford LFR Cameras



4.4.3. Capacity to Refuse or Withdraw Consent Without Penalty

A controversial issue, and one that gave rise to significant public debate, concerns police interactions with those individuals who refused or withdrew consent. This specifically concerns police interventions with people who turned around, covered their faces, or otherwise refused to walk past the cameras.[290] Policies for intervening with individuals avoiding the cameras changed during the course of the test deployments. The issue itself also grew in significance in public debates on LFR and generated the most contentious issues for intervention teams during the final two deployments at Romford.

An attempt was made to address the issue during the Stratford test deployments. However, there was considerable ambiguity surrounding this policy at the Stratford trials. During pre-trial briefings it was explained to officers that an individual turning around and refusing to walk past cameras was 'not an indicator of suspicion' in itself.[291] The explicit reason given was that this formed part of an individual's right to privacy. However, this was then re-framed: a 'turnaround' was argued to constitute evidence of LFR working as a 'crime disruption strategy' (rather than an individual protecting their own rights to privacy or refusing to offer their biometric information). This re-framing in turn facilitated an interpretation of refused consent as grounds for suspicion, and hence possible intervention under

[290]Discussion here is also developed in later sections where interventions of police on the ground are fully discussed. See Section 4.9.
[291] Briefing statement 26/7/2018.

ordinary police powers. At the very least the overall message in the briefing was thus very much a mixed message

Briefings made ahead of the next two test deployments in Soho during December 2018 were less equivocal. Officers were directed to consider stopping individuals deemed to be 'intentionally' avoiding the camera's zone of recognition. Discretion was advised in deciding what type of avoidance behaviour should count as 'intentional' and the degree to which it could be considered suspicious. This question was followed up with field officers who explained the role of experience and professional discretion in making such judgements. When asked again about this issue in a post-operation debrief, researchers were informed that there had in fact been no police interventions with individuals avoiding the cameras.[292]

Discretion and experiential knowledge are universally regarded as important features of policing. Indeed, it is important to recognise that opponents of algorithmically informed policing consistently argue for the retention of police discretion as a key safeguard against machine bias.[293] It is notable that, according to information supplied by police to the researchers, no interventions with, or arrests of, camera avoiding individuals were made in Leicester Square, one of central London's busiest areas during a particularly busy pre-Christmas period, as part of the Soho trials. By contrast, the number of camera avoider interventions and arrests (four) in an area significantly less traversed – Romford town centre – at a much quieter time of year is striking. This discrepancy is strongly suggestive of disparities in the way discretion was exercised and points to a need to address this in order to maintain consistency of approach.

However, even where discretion might be seen as reasonably exercised, the overarching point remains that treating LFR camera avoidance as suspicious behaviour undermines the premise of informed consent. In addition, the arrest of LFR camera avoiding individuals for more minor offences than those used to justify the test deployments raise clear issues regarding the extension of police powers and of 'surveillance creep'.[294]

---

[292] This account is contested by observers from civil society groups, who claim to have witnessed police interventions on the basis of perceived camera avoidance during the Soho deployments. In an on-the-record interview, Big Brother Watch director Silkie Carlo stated, 'We saw that at Leicester Square [a Soho trial] as well. We saw a young man who was made late for work because where it was cold he'd put the scarf over his face and he was ID'd' (interviewed 5 March 2019). The debrief took place very shortly after the test deployments and one explanation could be that all information from all parts of the police had yet to be collated. However, the disparity in accounts remains.

[293] e.g. Joh, E. (2016). 'The New Surveillance Discretion: Automated Suspicion, Big Data, and Policing'. *Harvard Law & Policy Review*, 10, 15–42; O'Neil, M. (2016) *Weapons of Math Destruction: How big data increases inequality and threatens democracy*, London: Allen Lane.

[294] 'Surveillance creep' is a term popularised in the 1980s by MIT professor Gary Marx (Marx, G. (1989) *Undercover: Police surveillance in America*, Oakland, CA: University of California Press) and has since acquired mainstream use. In essence, the term refers to the way surveillance measures justified for one particular purpose become repurposed for another.

The approach to turnarounds was refined in two distinct ways for the Romford test deployments in January and February 2019. First, greater stress was placed on the role of discretion in relation to people avoiding the camera zone of recognition, with no mention of 'intentional', as opposed to non-intentional, avoidance. Officers were instructed that individuals *may be considered* for an identity check if officers *felt* the behaviour could be considered suspicious. It is noteworthy that this heightened emphasis on discretion accompanied an increase in engagements with camera avoiders. The second difference, and one that was to prove significant, was that the Romford deployments were the first to utilize handheld devices in a consistent way. The Romford briefing pointed to the role of mobile devices[295] in confirming the identity of individuals, not only when they were stopped on the grounds of a LFR match but also if stopped on the basis of behavioural cues when avoiding cameras. Since the mobile handheld devices also had access to alerts and the watchlist, this meant that intervention teams had the capacity to use their discretion to match individuals against the watchlist independently of the intelligence teams in the control room.

Eight individuals were arrested during the first Romford trial (31 January 2019). Two of these arrests occurred as a direct result of LFR alerts concerning a match of individuals walking past the cameras to the watchlist and adjudicated as credible.[296] However, the other six arrests were related to the LFR test deployments but did not occur as a result of a match made by van-based LFR cameras. The circumstances of these arrests are highly significant in assessing the operation, reach, and proportionality of LFR as well as issues of consent. The details of each arrest are set out below.

Romford Arrest 1/6. The account of this arrest given at the time, and one confirmed again to the researchers during follow-up enquiries, is that an individual put their hood down to conceal their face as they walked past the LFR cameras. This was considered a suspicious response by the officer, who then engaged with the individual. A handheld device was then used to check the subject's face against the watchlist. A positive match was returned with the subject wanted for a serious offence and subsequently arrested.[297]

Romford Arrests 2/6 and 3/6. Two individuals were apprehended for shoplifting by private security guards in a nearby shopping centre, outside the camera zone of recognition, and beyond the range of communication between the LFR van and

[295] Mobile devices are discussed in more detail in the section on adjudication and intervention below, section 4.8.1. Mobile devices were issued at all observed test deployments but only really utilised during the Romford trials. During the Romford trials these handheld devices had two main capabilities: (1) alerting street-based intervention team officers to a computer-generated match (2) a camera in the device that could capture facial images and compare to the watchlist.

[296] Stops six and seven on Table 4.9.

[297] This arrest is not included in the analysis of alerts and outcomes for this trial (Table 4.9.). This is because the stop was not initiated by the LFR cameras. LFR camera-initiated interventions is the variable being analysed by the tables.

handheld devices. A call for assistance was issued by the shopping centre guards and an officer assigned to the LFR test deployment responded. This investigating officer was equipped with a handheld device. The device was then used to check the identities of the two suspected shoplifters against the watchlist. Officers then reported that, based on further enquiries, these individuals were listed on CRIS (a more intelligence-focused database) but the information had not been uploaded onto the Emerald Warrant Management System (the database of wanted individuals, i.e. those with warrants out against them). They were therefore not on the watchlist but were nonetheless arrested in relation to their alleged activities in the shopping centre that morning. This information is included in the report because it relates to an active use of the LFR capability.

Romford Arrests 4/6 and 5/6. Two individuals were reported to have walked past the information boards and then immediately ran down a side street. They were pursued by officers, stopped and searched. They were subsequently arrested for drug-related offences.

Romford Arrest 6/6. An individual was searched after avoiding the LFR van and subsequently arrested for drug-related offences.

Another pertinent incident during the Romford trials, captured in the national media,[298] relates to an individual who avoided the camera and was subsequently issued a £90 fixed penalty fine on the grounds of a public order offence. The circumstances surrounding this incident are contested. A perspective was sought from MPS Officers and a response received from commanding officers following their review of video footage from police body worn cameras. One of the researchers also viewed independent (unreleased) media video footage of the incident. The eyewitness account from civil society observers is:

> So, the first day in Romford, a man was actually fined for having a scarf over his mouth and chin, and then goaded by police. And then he said an expletive, apparently. I didn't hear it, but apparently he did and then he was given a Public Order Fine of £90.[299]

The national media story consists of an almost verbatim repeat of the views expressed by the same civil society observers on Twitter. The police interpretation of the incident is that the individual arrested became aggressive and abusive to officers when confronted, and the public order fixed penalty was issued in accordance with standard procedure for addressing such behaviour. The independent (unreleased)

[298] Lizzie Dearden, 'Police stop people for covering their faces from facial recognition camera then fine man £90 after he protested', *The Independent*, 31 January 2019, Available at: https://www.independent.co.uk/news/uk/crime/facial-recognition-cameras-technology-london-trial-met-police-face-cover-man-fined-a8756936.html.

[299] Interview with Silkie Carlo, Director, Big Brother Watch.

media video footage reveals an escalating confrontation between this individual and the police intervention teams.

It is beyond the scope of this report to assess the propriety of police responses to alleged public order incidents. However, this episode raises two considerations relevant to the public trialling of LFR. First is the degree to which this trial cultivated the circumstances leading to this heightened conflict and the extent to which this should be taken into account by officers when deciding on an appropriate response. Second, the independent media footage shows the matched individual having his photograph taken with a handheld face recognition equipped device early on in the engagement. While the officer mentions he is taking the individual's photograph while triggering the shutter, there is no meaningful dialogue between the two people, and no indication of consent given. While this was not an issue of consent in relation to the LFR *camera*, this person's details were then compared against the watchlist and no match was discovered.

An added theme is also pertinent to the difference between a trial for research purposes and an active police deployment, as discussed in Section 1.2.3. The first Romford trial ended ahead of schedule, at around 4:30pm. This was because officer numbers had been critically depleted by the numbers attending to arrests of people refusing to walk past LFR cameras. In this sense, LFR-related policing aims took primacy over 'trialing' of the technology.

4.4.4. Consent to Research and Consent to Police Operations

These consent issues again evoke debates over the twin themes of LFR as active deployments versus conducting trials in accordance with standards of research ethics. From the perspective of research ethics, someone avoiding the cameras is an indication that they are exercising their entitlement not to be part of a particular trial or are protecting their own right to privacy. Analogies would be an individual choosing not to take part in some other form of research, such as a marketing survey or medical trial, and this would be the expected norm for the treatment of volunteer subjects in a social science or psychology experiment. In addition, privacy preserving behaviours are commonplace across society and common sense in many contexts. In these settings it would be a breach of research ethics to penalise people for protecting their individual rights. From a policing perspective, this same behaviour may acquire a different meaning and serve as an indicator of suspicion. While this tension may apply to other trials of police equipment, it is particularly acute in the case of LFR given its intrusive nature, and requires urgent attention for future testing of this technology (as well as other technological innovations).

The argument that, if such experiments are justified on the basis of trialling then they are beholden to the standards that apply to other forms of trial (such as medical or

other research), is compelling. This point was also raised by the London Police Ethics Panel[300] during their 2018 review of LFR:

> To the extent that the trials are akin to field research, they should be governed by the ethical precepts that apply to research. As we noted above, the conventional basis for engaging participants in research is either through consent; or a compelling justification for dispensing with consent, generally requiring the research to be in the interests of each individual involved.[301]

With specific reference to consent, such standards offer an available ethical vocabulary and a clear set of standards relevant to the trialling of such tools.

Consent also links to other areas of consideration. Among these, the arrest of LFR camera avoiding individuals for more minor offences than those used to justify the test deployments raise clear issues regarding the extension of police powers and of 'surveillance creep'.[302]

4.5.From Alert to Resolution

This section outlines the envisaged sequence of events, from an LFR-generated alert onwards. Subsequent sections discuss how this process happens in practice:

Alert ➔ Adjudication ➔ Engagement ➔ Confirm identity ➔ Action

There are two key moments in this process: (a) adjudication, in which computer generated matches of individuals' images are reviewed by intelligence officers, and (b) the identity checks conducted by the intervention team on the street. These are crucial moments both from the 'research' perspective and the human rights perspective in which the strengths and weaknesses of this 'socio-technical system'[303] are most crucially manifested. Many of these concerns ultimately turn around 'false positives' arising from computer-generated matches. These may be potentially corrected by the human adjudication process and are subject to a final check when police seek to confirm the putative identity of a member of the public as a person on the watchlist.

At the same time, these processes have a different register when viewed in terms of legal and regulatory requirements, as will briefly be outlined here.

---

[300] The independent panel established by the Mayor of London to provide ethical guidance on police issues in the capital.

[301] London Police Ethics Panel (2018) Interim Report on Live Facial Recognition, London, London Police Ethics Panel, p.10, available from http://www.policingethicspanel.london/uploads/4/4/0/7/44076193/lpep_report_-_live_facial_recognition.pdf

[302].See footnote 294.

[303] Davies et al. (2019) South Wales police report p6

4.5.1. Computational Processing and Human Intervention

The initial stages of the LFR operation is entirely based on automated processing which seeks to match a 'captured' (or 'probe) image of persons at the scene against images on the watchlist ('gallery image'). Whether matches are found depends in part on the 'similarity setting', by which the algorithms are set to identify matches based on a selected threshold of similarity. For all observed MPS LFR test deployments the threshold (also sometimes called the score setting) was set at 0.55. The lower the threshold is set the more matches will be found but the less accurate those matches are likely to be. The opposite is also true, a higher threshold yields fewer matches but there is a higher degree of confidence in their accuracy.

An alert is generated by the LFR technology when a match is found. The alert goes to the adjudication operator(s) along with the images. It is at this point that a key element of human contribution occurs: a judgement as to the credibility of the match (adjudication). In the observed test deployments, this central filtering was conducted primarily in the control room. Here the operator, ideally someone with training and/or a member of the intelligence team, makes a judgment stated to be 'on the balance of probability' (the civil standard of proof) as to the credibility of the match, looking at the two images and deciding whether to accept or discard the match.

There are a number of reasons for interposing this human element into the otherwise automated process. In particular, section 49 of the Data Protection Act holds that a 'significant decision' concerning a particular individual may not be made exclusively on the basis of an automated decision (i.e. some form of human adjudication is required) 'unless that decision is required or authorised by law.'[304] Considerations of accuracy, efficacy and efficiency are also brought into play.

The role of meaningful human intervention has been underlined since the first iteration of the Surveillance Camera Code of Practice:

> Any use of facial recognition or other biometric characteristic recognition systems needs to clearly justified and proportionate in meeting the stated purpose, and be suitably validated. *It should always involve human intervention before decisions are taken that affect an individual*.[305]

This is developed in recent guidance specific to the use of face recognition (published after the Metropolitan Police test deployments concluded),

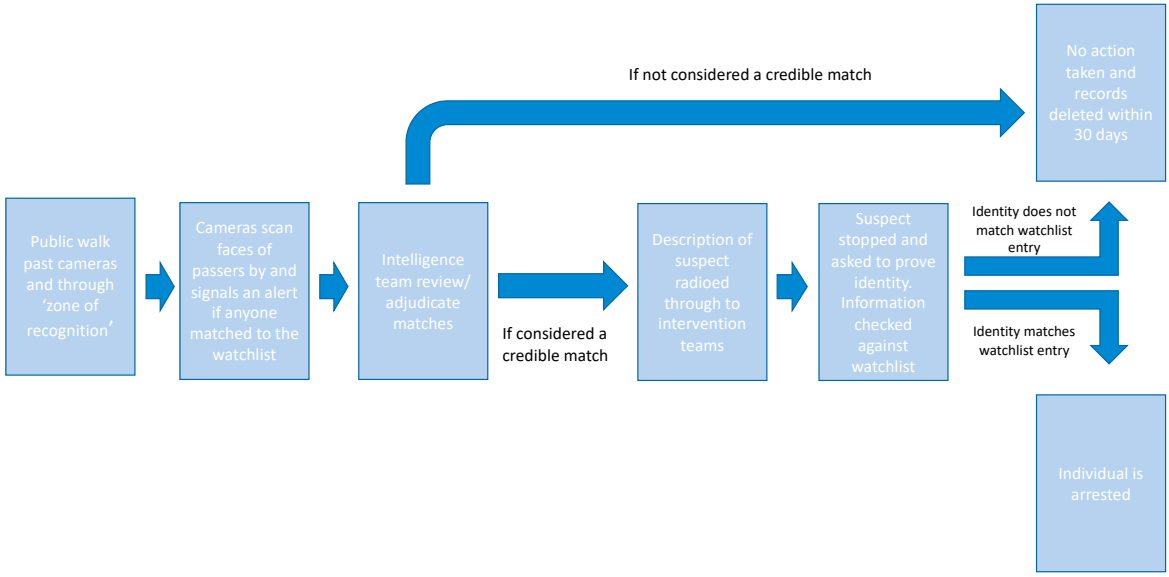
[304] Data Protection Act 2018, section 49. This section reads in full: '(1) A controller may not take a significant decision based solely on automated processing unless that decision is required or authorised by law. (2)A decision is a "significant decision" for the purpose of this section if, in relation to a data subject, it— (a) produces an adverse legal effect concerning the data subject, or (b) significantly affects the data subject.'

[305] Para 3.2.3, Surveillance Camera Code of Practice, 2013 emphasis added.

> The AFR technology and algorithms employed are but one ingredient of a 'full system approach' to deployment and regulation of a surveillance camera system. A fundamental requirement of the SC Code and any operational deployment of AFR is that there must be human intervention within final decision making. These systems are devised to alert operators to potential individuals of interest for human operators to review. They are a tool in a process; the overall process requires human intervention and it is this overall process that requires validation[306]

Accordingly, if the match is accepted and deemed credible, this decision along with a description of the matched-individual would then be conveyed by radio to intervention teams stationed nearby. A complicating issue concerns the use of mobile devices issued to street-based intervention teams, discussed below.[307] Once engagement is flagged in this way, police on the ground will then try to locate the person who was matched by the system.

Fig. 4.6. Diagram of Indicative LFR Adjudication Process and Identity Check[308]



Identity checks were accomplished through a number of means. Most often this involved the production of a standard identity document. If this was not offered, officers used mobile fingerprint scanners ('Mobile Ink' technology). If matched

[306] Surveillance Camera Commissioner (2019) *The Police Use of Automated Facial Recognition Technology with Surveillance Camera Systems*, 11.3 p.10 available from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/786392/AFR_police_guidance_of_PoFA_V1_March_2019.pdf

[307] See Section 4.7.2.

[308] This is a diagram of an indicative process, not a description of formal procedure.

[309] Articulated at pre-deployment briefings.

individuals refused to have their fingerprints taken in the street, as occurred at one of the Romford test deployments, officers were then given the option of arresting and escorting individuals to a police station for additional identity checks.

4.6. Detailed Analysis of Alerts: Adjudication and outcomes

Adjudication was a consistent feature of the observed test deployments. Variations in adjudication procedure existed between each test deployment. LFR matches were only overturned by adjudicators for the first time almost midway through the third observed test deployment in Soho (17th December 2018).

Five alerts were generated at the first Stratford trial. The first (at 15:12) can be discounted because the intervention team were not yet assigned and there was no capacity to respond to the alert. The remaining four alerts were adjudicated to be credible, sometimes immediately. In each of the four cases, either the intervention team or members of the intelligence unit monitoring the cameras in the control room engaged with the individual matched by the system. On the basis of the identity confirmation checks by the intervention officers, all four were verified incorrect matches (the first discounted match could not be determined as no engagement occurred).

At the second Stratford test deployment only one alert was generated by the LFR technology during the 10 hours of the trial. This was adjudicated to be a credible match in the control room and the intervention team was requested to engage the subject. The person was initially lost in the crowd but later picked up by shopping centre security cameras. When identity checks were carried out, this resolved as a verified incorrect match.

In relation to the subsequent test deployments in Soho and Romford, **Tables X-X** detail the alerts,[310] adjudication decisions, outcomes in respect to on the ground identity checks and subsequent action, plus any additional relevant information.

- 'Alerts' refers to matches made by cameras linked to the control centre where adjudications were made. This excludes matches made independently by

[310] A note on counting: All stops have been cross referenced with the MPS LFR technical evaluation team. The researchers have also adopted the MPS method of counting in order to aid comparison across the reports. The MPS technical evaluation team count the number of matches to *different individuals on the watchlist*. If an individual is matched against a duplicate watchlist record (e.g. alert 12, table 4.10, second Romford test deployment), this is counted as one alert. However, two anomalies exist:

1. The MPS have chosen to count an occasion when an individual was matched against two different watchlist records as *one match* (match 5, table 4.10, second Romford test deployment). The researchers have adopted the MPS statistics for this table;
2. One individual was matched as a true positive (match 5, table 4.9, first Romford test deployment). The same individual walked past the cameras a second time later that afternoon and triggered a second alert (match 8, table 4.9, first Romford test deployment). This match is included in the MPS technical evaluation statistics so is retained in this description of alerts here. This match is not included in the calculation of verified correct/incorrect matches in Section 4.1. above because it double counts an existing verified correct match and is not related to a police intervention.

street-based officers using handheld mobile devices, evidently an issue in need of further discussion (see section 4.8.1). This issue occurred only at the Romford test deployments. The mobile devices used at Romford were able to receive actual alerts and hence actual images, as well as take photographs of individuals for comparison against the watchlist.

- 'Algorithm similarity score' refers to the value given by the LFR system. This value falls between zero and one, and is set manually as per the manufacturer's threshold at 0.55. Somewhat simplifying, the similarity score can be understood to denote the degree of similarity between the probe and gallery images calculated by the computer. A high number broadly signifies the computer calculating a high level of similarity between the images. Scores below the 0.55 threshold would not generate an alert on the main LFR system.
- 'Principal site of adjudication' relates to where the decisive adjudication took place. In the initial test deployments principal adjudication occurred in the control room. In later test deployments, images were reviewed by intelligence units in the control room and intervention teams equipped with mobile devices on the street. Sometimes adjudication occurred in both places simultaneously. This column notifies where the conclusive decision to ignore or take action on the basis of an alert took place.
- 'Outcome of human adjudication' refers to MPS officer decisions over whether a computer generated match was deemed credible or non-credible. As the discussion below relates, some matches did not fall neatly into either of these categories. In these circumstances, the outcome of the adjudication process was viewed as a 'credible match' if a decision was taken to intercept a matched individual. N/a denotes both 'not applicable' and 'indeterminable'. Based on the definition adopted above (see section 4.1.3), a match is not verified unless it was companioned with a physical identity check with the individual suspected of being on the watchlist.
- The 'intervention or attempted intervention' column details any attempt to engage with an individual matched by the LFR system. Some attempts to find matched individuals were unsuccessful (e.g. they were absorbed into crowds). Some interventions also occurred after a decision had been made to overrule a LFR system match. This was particularly prevalent when officers outside the control room were alerted to matches on their handheld devices and elected to intervene. Because the analysis here is focused on decision-making related to LFR suggested matches, all decisions to intervene are recorded.

Table 4.7. Analysis of LFR Alerts and Outcomes, First Soho Test Deployment, 17th December 2018

Alert number	Time of alert	Algorithm similarity score	Principal site of adjudication	Outcome of human adjudication	Intervention or attempted intervention with matched individual	Type of intervention	Outcome of intervention	Other relevant details
1	11:24	0.55	Control room	Credible match	Yes	Individual stopped and identity checked	False positive. Individual wanted for non-watchlist reasons. Subject Arrested.	Identity confirmed with mobile fingerprint scanner. Subject was wanted for offences different to those eligible to be enrolled on the watchlist.
2	13:20	0.56	Control room	Credible match	Yes	Individual stopped and identity checked	True positive. Subject Arrested.	Matched individual claimed the offence listed on the watchlist had been dealt with by the criminal justice system. Police National Computer checks revealed the individual was wanted in relation to malicious communications (a lesser offence)*
3	13:28	0.56	Control room	Non-credible match	No	No action taken	n/a	First incidence of computer generated match deemed non-credible and no action taken, in any of the observed test deployments
4	14:22	0.57	Control room	Credible match	Yes	Individual stopped	False positive. No further action	Radio and tablets not working. Officer left van to pursue matched individual on foot. Very fast adjudication decision to take action.
5	14:26	0.58	Control room	Non-credible match	No	No action taken	n/a	

*More details of this case are given in the discussion of watchlists above. Counted as a verified correct match because the computer decision was verified as correct with an identity check (although the input data was outdated).

Table 4.8. Analysis of LFR Alerts and Outcomes, Second Soho Test Deployment, 18th December 2018

Alert number	Time of alert	Algorithm similarity score	Principal site of adjudication	Outcome of human adjudication	Intervention or attempted intervention with matched individual	Type of intervention	Outcome	Other relevant details
1	10:48	0.59	Control room	Non-credible match	No	No action	n/a	
2	11:16	0.55	Control room	Non-credible match	No	No action	n/a	Wrong gender
3	11:24	0.58	Control room	Non-credible match	No	No action	n/a	Wrong gender
4	11:54	0.55	Control room	Non-credible match	No	No action	n/a	Gallery (file) image older than probe image
5*	13:00	0.63	Control room	Credible match (some deliberation but match deemed sufficiently credible to attempt an intervention with the matched individual)	Yes	Individual stopped and identity checked	True positive. Subject arrested	Technical difficulties as the system would not enlarge the picture. One officer leaves the van quickly to intercept the subject. Others in the van still deliberating and started to reach a conclusion that it probably was not a match due to age difference. By this time the subject had been stopped and an identity check performed, which confirmed the individual as wanted.
6	13:34	0.58	Control room	Non-credible match	No	No action	n/a	
7	13:50	0.55	Control room	Credible match (some deliberation but match deemed sufficiently credible to attempt an intervention with the matched individual)	Yes	Individual lost in the crowd	n/a	Subject's clothes are out of frame. This makes it impossible to provide intervention teams with a detailed description. Individual could not be traced.
8	15:44	0.58	Control room	Credible match (some deliberation but match deemed sufficiently credible to attempt an intervention with the matched individual)	Yes	Individual lost in the crowd	n/a	
9	15:45	0.56	Control room	Non-credible match	No	No action	n/a	Gallery (file) image older than probe image

* The same individual generated two separate alerts at roughly the same time. For the purposes of clarity, dual matches are treated as a single alert if one individual is matched against the same watchlist record at around the same time. See fn 310 above.

Table 4.9. Analysis of LFR Alerts and Outcomes, First Romford Test Deployment, 31st January 2019

Alert number	Time of alert	Algorithm similarity score	Principal site of adjudication	Outcome of human adjudication	Intervention or attempted intervention with matched individual	Type of intervention	Outcome	Other relevant details
1	09:53	0.59	Control room	n/a alert occurred before intervention teams deployed at the start of the trial	No	No action	n/a	Alert occurred while technical team were setting up. Match discounted from the analysis.
2	10:02	0.56	Control room	Non-credible match	No	No action	n/a	
3	10:09	0.55	Control room	Credible match	Yes	Individual stopped and identity checked	False positive	
4*	11:20	0.57	Control room	Credible match (some deliberation but match deemed sufficiently credible to attempt an intervention with the matched individual)	Yes	Individual lost in the crowd	n/a	Some adjudication in the van. Technical difficulties and mobile device was not working correctly. Difficult to find individual on the basis of descriptions (black coat and fur hood on the coldest day of the winter). Adjudicated as a non-credible match in the final instance but only after prior unsuccessful attempt to intervene
5	14:30	0.69	Control room	Credible match	Yes	Individual stopped and identity checked	True positive. Matched individual no longer wanted. No action taken.	Blurred probe image but a true positive. Out of date watchlist. Individual had been processed by the criminal justice system and was no longer wanted.
6	14:57	0.61	Control room	Credible match	Yes	Individual stopped and identity checked	True positive. Subject arrested	
7	15:47	0.68	Control room	Credible match	Yes	Individual stopped and identity checked	True positive. Subject arrested	
8**	15:48	0.68	Control room	Credible match but individual previously stopped (at 14:40)	No	No action	True positive but no action taken.	Second match of same individual from alert #5. True positive but out of date information. Repeated match, discounted from the analysis.
9	15:59	0.59	Control room	Credible match	Yes	Individual stopped and identity checked	False positive	
10	16:16	0.56	Control room	Non-credible match	No	No action	n/a	Trial ended 16:30 due to depleted numbers of officers

*As discussed below, another arrest occurred between alerts three and four, at 10:20am. This occurred because an officer equipped with a handheld device photographed an individual seen to be avoiding the camera's zone of recognition. This is not counted in these tables because the focus is on computer-generated matches.

** See fn. 310 above. There is an argument to delete this record because it does, in effect, represent a duplicate match with *the same watchlist record* (match 5). It is similar in nature to match 12 in the second Romford test deployment (14/2/2019, see Table 4.10 below), differing in the time between alerts. However, this match is included in the MPS technical evaluation statistics so is retained in this description of alerts here. This match is not included in the calculation of verified correct and incorrect matches in this report (Section 4.1.3 above) because it duplicates (or double counts) an existing match and is not related to a police intervention.

Table 4.10. Analysis of LFR Alerts and Outcomes, Second Romford Test Deployment, 14th February 2019

Alert number	Time of alert	Algorithm similarity score	Principal site of adjudication	Outcome of human adjudication	Intervention or attempted intervention with matched individual	Type of intervention	Outcome	Other relevant details
1	10:29	0.57	Control room	Non-credible match	No	No action	n/a	Alert occurred as system was being set up. Match discounted from the analysis.
2	13:32	0.58	Control room	Non-credible match	No	No action	n/a	
3	13:53	0.55	Control room	Credible match	Yes	Individual stopped and identity checked	False positive	
4	14:55	0.83	Control room	Credible match	Yes	Individual stopped and identity checked	True positive. Subject arrested	Alert did not transmit to mobile devices. Officer set out from the van to communicate the match
5*	15:19	0.55/0.56	Control room	Non-credible match	No	No action	n/a	Same individual matched against two different gallery images (counted by MPS as one match)
6	15:27	0.56	Control room	Credible match	Yes	Subject lost in the crowd. Subsequently adjudicated and decided it was not her.	n/a	Disagreement in the van over whether to intervene. Radioed through for intervention. Policy developed that when opinion was split in the van the approach was to intervene.
7	15:28	0.60	Intervention team with handheld	Credible match	Yes	Individual stopped and identity checked	False positive	Insufficient capacity to deal with this because they were processing the previous match that occurred minutes before. Insufficient resource to radio through. However, individual stopped by an officer with a tablet and alerted to the match.
8	15:31	0.56	Control room	Non-credible match	No	No action	n/a	
9	15:47	0.55	Control room	Non-credible match	No	No action	n/a	
10	15:48	0.60	Control room	Non-credible	No	No action	n/a	Different ethnicities

				match				
11	16:00	0.56	Intervention team with handheld	Credible match	Yes	Individual stopped and identity checked	True positive. Subject arrested	Double hit from same image. Same matched individual triggered two alerts. Adjudicated as non-credible in the van but matched individual stopped by intervention teams.
12**	16:16	0.61 + 0.57	Intervention team with handheld device	Credible match	Yes	Individual stopped and identity checked	True positive. Subject arrested	Individual stopped by intervention teams while officers in the van deliberating.
13	16:18	0.58	Control room	Credible match	Yes	Individual stopped and identity checked	False positive	
14	16:31	0.56	Intervention team with handheld device	Credible match	Yes	Individual stopped and identity checked	False positive	
15	17:01	0.61	Control room	Non-credible match	No	No action	n/a	
16	17:12	0.57	Intervention team with handheld device	Credible match	Yes	Individual stopped and identity checked	False positive	

*The same individual generated two separate alerts at roughly the same time. As noted in footnote 310, the MPS technical evaluation team count the number of matches to *different individuals on the watchlist*. The researchers have adopted the MPS method of counting to facilitate clarity and comparison across different reports.
**This individual was matched against two records (for two separate offences) of the same person on the watchlist. The MPS technical evaluation team count this as one match. The research team have adopted their counting rules for this analysis.

4.7. Adjudication

In total, over the six observed test deployments, the LFR technology matched 45 individuals at the scene to individuals on the watchlist. 16 of these matches were deemed non-credible and rejected, and thus no police engagement was attempted at the scene.

Adjudication processes evolved and shifted across the test deployments. It is important to note that these shifts in practice also occurred in the context of other changes, such as increases in watchlist sizes, different availabilities of support teams, diverse geographical settings and inconsistent performance of communications technology.[311]

The theme of increasing officer ability to use LFR as operational experience develops is highlighted in other studies.[312] As the test deployments progressed,

[311] See section 4.8 below where these contextual features are considered in more depth.
[312] Bethan Davies, Martin Innes and Andrew Dawson (2018) *An Evaluation of South Wales Police's Use of Automated Facial Recognition*, Cardiff: Universities' Police Science Institute, Crime and Security Research Institute, Cardiff University.

operators/intelligence team members manifested a growing confidence in their ability to make an appropriate discretionary judgment 'on the balance of probability'.

The first adjudication to overrule a computational match occurred midway through the third observed test deployment.[313] This was judged as a non-credible match on the basis that the computer captured live image corresponded to the image of a much older female on the watchlist. The rate of disconfirming alerts became more frequent following this initial occurrence.[314]

4.7.1. Recognising the value of the adjudication process

All observed officer briefings were clear on the importance of human discretion in the LFR process. Particularly common and consistent across all briefings was the instruction that:

> the generation of an alert is never treated as a sole indication that a positive match has been secured. Officers are expected to conduct further checks to confirm their [the matched individual's] identity including the use of INK technology [for on the spot fingerprinting].

Officers were therefore instructed that a computer derived match was not sufficient to confirm an identity in and of itself. This is appropriate given the significant error rates associated with LFR. Paradoxically, statements recognising the valuable role of human discretion – 'human engagement is critical' and 'generation of an alert should never be treated as a sole indicator of suspicion' – were regularly accompanied with testaments to the powerful capability of LFR technology. For example, in two operational briefings this message was companioned with statements that, 'it is 100% effective in spotting those uploaded into the system' (MPS Officer 28 June 2018) and 'the technology is very accurate, despite misinformation' (MPS Officer 24 July 2018). Such mixed messages potentially undermine the important emphasis on human adjudication. Nor did they reflect the more nuanced views of those actually operating the technology. This overconfidence in the accuracy of LFR technology was particularly prevalent at earlier test deployments and less in evidence towards the end of the process.

A perhaps parallel phenomenon can be seen in respect to so-called 'super-recognisers'.[315] The potential for using 'super recognisers' in the adjudication process

[313] Alert 3 of the first Soho test deployment, 17th December 2018, Table 4.7.

[314] See Section 4.7.2on handheld devices for instances where control room decisions were overruled by the intervention team.

[315] 'Super recognisers' refers to a category of police officer judged to hold above-average abilities in identifying facial characteristics and matching images of the same face across different media. Within the Metropolitan Police Service, the role of super recognisers developed significantly following the 2011 riots in England where video footage was intensively analysed to identify specific individuals. Now formalised training, accreditation and status attach to the super-recogniser role in the

was aired repeatedly through the test deployments, and some super recognisers were deployed during the LFR test deployments although their role was focused on street-level intervention rather than adjudication within the control room. Should the role of 'super recognisers' be considered going forward, it is important to note that while some people arguably have a greater ability to match faces than others[316] – which may assist in the investigation of crime – the Forensic Science Regulator has considered their role in her annual reports for 2017 and 2018, following the collapse of a legal case in which evidence from a 'super recogniser' was deemed flawed. Her view is that their work certainly does not have a satisfactory basis to count as part of forensic science as such.[317] Regarding 'the use of the output from the work as evidence', she suggests strengthening the Police and Criminal Evidence Act 1984 (Code D) where it deals with recognition in relation to the identification of suspects.[318]

4.7.2. Variations in Adjudication Practice

Adjudication practices varied across the deployments, these can be placed within three distinct categories and are discussed in turn.

(1) Multiple adjudicators in the control room

The intelligence teams reviewing LFR footage varied in number and location. While there were times when one officer was stationed in the control room monitoring the screens, the usual practice was to involve more than one individual as 'operators' in the adjudication process. Multiple operators brought additional scrutiny to the process but also raised the likelihood of contrasting approaches within the same adjudication team.

During one Soho trial two adjudication operators were monitoring the same screen when the system made an alert. One of the officers commenced a deliberation and, in the end, decided that, on balance, this was not a credible match owing to the evident age disparity between the two images. The other officer, however, had meanwhile already left the van and apprehended the matched individual while this deliberation was taking place (the radio communications were also operating poorly). In addition to highlighting disparities in the adjudication process, this incident contrasts with the indicative process in which operators and intervention officers comprise two distinct roles. Other examples concerning multiple roles can be found below in section 4.8.1. In this instance the match proved to be the only verified

investigation process. Several commercial consultancies also offer super recogniser services. It is important to note that MPS officers and staff expressed a range of perspectives to the researchers over the benefits of super-recognisers.

[316] Proponents of super recognition appeal to scientific evidence drawn from the field of applied psychology: see, for example Valentine and Davis 2015.

[317] It 'is not based on scientifically validated methodology, nor are error rates known', Forensic Science Regulator (2018: 20).

[318] Forensic Science Regulator (2019: 32). It is also interesting to note accounts from MPS staff, expressed to researchers, claiming a progressive reduction of the role of super recognisers and renaming as 'identification officers' in the constabulary.

correct match of the second Soho test deployment and resulted in the matched individual's arrest. Yet this result does not justify such pre-emptive action in all circumstances. If this precipitate action had been repeated across the day, such a level of trust in the algorithm would likely have been misplaced, given that every other computer generated match had been incorrect or adjudicated as non-credible.

(2) Simultaneous adjudication and street engagement

Another variation on this process occurred when van-based intelligence units and street-based intervention teams operated simultaneously rather than sequentially. This involved intelligence officers radioing through a description of a LFR match *while they were still in the process of deliberating over the credibility of the alerted match*. A decision to trigger the street intervention team to start looking for the matched individual may arguably have been based on sound operational reasons. It bought intelligence officers important 'thinking time' while under pressure to make a rapid decision and it allowed the intervention team to start looking for the matched individual before losing sight of them.

As discussed below in section 4.8.2, this sort of decision making reflects the challenges of particular physical geographical settings and the associated time pressures. A difficulty with this approach, however, is that it indicates a discernible 'presumption to intervene'.[319] This was not an isolated example. Every instance in which this simultaneous approach was followed led to an attempt to engage a matched individual. This includes instances when intelligence units ultimately adjudicated that the LFR system had not supplied a credible match. As such, greater clarity is possible over whether communications to intervention teams are instructions to maintain observation or an instruction to intervene.

(3) Mobile devices and simultaneous adjudication on the street and in the control room.

In the Stratford and Soho test deployments tablet-sized devices were issued to members of the intervention team on the street. Technical failures and limited street-based officer use of these devices left them largely idle during the Stratford and Soho test deployments. The devices were replaced with smaller smart-phone sized devices in the two Romford test deployments, where they were used extensively.

These handheld devices had the capacity to receive alerts and access the watchlist. How this operated needs to be explained more precisely to understand the implications of their use.

Computer-generated alerts were sent simultaneously to the adjudication operators in the control room and to the intervention team's handheld devices. Alerts sent to

[319] Also see below, section 4.8.

the adjudication operators were based on a threshold score setting (as described above) set at 0.55 in conformity with the manufacturer's recommended specifications. Mobile handheld devices did not have this threshold functionality. Instead, the handheld devices used by the street-based intervention team showed a range of matches not limited to the 0.55 threshold, with those matches attaining the highest confidence score at the top of the list. Additional watchlist records were also displayed including those below the established threshold score.

Various potential uses of these devices were expressed. Combined with observations of their use in practice, two discernible and distinct possible uses by the street intervention team can be identified. These were:

(i) assisting street based intervention teams in the location of matched individuals.
As outlined above, according to the indicative adjudication process, once a computer generated match was adjudicated as credible, intelligence teams would radio through a *verbal description* to street based intervention teams who would then seek to intercept the matched individual. One intended purpose of issuing handheld devices was so that intervention teams had access to *actual images* of the persons they were expected to seek out at the scene.

(ii) as an additional step in the adjudication process otherwise carried out by the control room operators.
It was repeatedly explained that control room intelligence teams were intended to be the primary decision makers in the adjudication process. To supplement this, handheld devices were also intended as a second point of adjudication in the process. The intention here was to provide a further 'check' on the original decision by intelligence units that the LFR match was credible. Intervention teams would be able to judge for themselves by comparing the computer matched image with a physical comparison of the subject they were observing on the street. While open to some interpretation, this purpose is also set out in the 'Metropolitan Police Service Live Facial Recognition Trial Evaluation Methodology'[320] supplied to the researchers. There was extensive use of handheld devices for this purpose during the final test deployment in Romford (14/2/2018). This use of mobile devices as a second stage of adjudication also aligns with the practice adopted during the South Wales Police trials of LFR.[321]

The practical use of mobile devices in this manner generated a number of issues that are important to note. In particular, while intended to add a second layer of discretion, this development of street-based adjudication questions the primacy, and

[320] 'MPS Live Facial Recognition Trial Evaluation Methodology' p 3.
[321] Bethan Davies, Martin Innes and Andrew Dawson (2018) *An Evaluation of South Wales Police's Use of Automated Facial Recognition*, Cardiff: Universities' Police Science Institute, Crime and Security Research Institute, Cardiff University.

potential relevance, of the role of intelligence-based deliberations given the number of decisions made, and acted upon, independent from this original process.

Street-based intervention teams equipped with handheld devices received alerts at the very same time that the intelligence units, the intended primary decision makers, stationed in the control room. This triggered adjudication processes *in both places at the same time*. Moreover, street-based intervention teams were receiving the same information and images in a far less filtered form.

During the second Romford test deployment, the decisive choice to intervene with a matched individual was made by street-based officers equipped with handheld devices on at least five occasions.[322] These mostly took place while intelligence units in the control room were deliberating over the credibility of a computer-generated match.

Decisions of the control room-based intelligence teams to engage a subject were never rejected by mobile-equipped officers. However, decisions by the primary adjudicators (control room-based intelligence units) not to intervene were frequently 'overruled' by street-based mobile-equipped officers on the basis of their separate access to imaging information.

Two cases of street-originated interventions transpired to be correct judgments of a credible match and led to the arrest of wanted individuals.[323] The other three occasions were incorrect matches *and* instances in which the original computational match had been adjudicated and discarded by the control room-based intelligence teams. Given the presumption in favour of intervention discussed earlier, and the time pressures of a live test deployment, it is reasonable to assume that technology failures impeded the likelihood of control room decisions in favour of non-intervention being overruled by mobile-equipped street-based teams during the Soho trials.

4.8.Contextual Factors Affecting Performance

LFR technology does not operate in isolation. It works in concert with a range of other technological, operational and geographical/spatial variables, each affecting the capability and outcome of LFR. Perhaps the most obvious of these is the element of time pressure, the fact that the use of LFR is live, happening in real time. Some of the effects of time pressure have already been illustrated above in respect to the adjudication process and street intervention (and further instances can be found below).

[322] Stops 7, 11, 12, 14 and 16 on Table 4.10.
[323] Stops 11 and 12 listed on Table 4.10.

4.8.1. Communications Technology

LFR is supported by other technological architecture in order to function correctly. Some of these issued have been discussed in relation to the use of handheld devices.[324]

Principal among these is communications technology that transmits LFR matched images to handheld devices and, separately, enables intelligence units (the operators conducting the adjudication process) to radio through a matched individual's details to street-based intervention teams. The ability to communicate descriptions of matched individuals is a core element of current LFR functionality.

During the second Soho trial the LFR system alerted operators to a potential match.[325] The probe (camera captured) image framed an individual's face as he passed through the bottom of the field of view. The rest of his body was out of frame. Combined with the technical failure in transmitting images to handheld devices, intelligence teams faced a near-impossible task of describing an individual's facial characteristics (a male in his 20s with blond hair) to intervention teams scanning a crowded pre-Christmas Leicester Square. This also points to a fallibility in LFR capability as this individual had previously walked across the entire field of view before being matched.

On other occasions, verbal descriptions made it difficult to isolate one individual from another. In these circumstances, officers complained of the challenges involved in compensating for the non-functioning mobile devices by providing verbal descriptions, given the difficult task of expanding on descriptions beyond 'female wearing a black coat with fur hood' – on the coldest day of the Winter.[326] These challenges reflect those encountered during LFR test deployments elsewhere. For example, the South Wales Police trials of LFR during Welsh international rugby matches encountered related difficulties, such as the challenge of providing differential descriptions of individuals dressed in red rugby jerseys.[327]

Technical difficulties affecting communications systems had another important influence on the adjudication process. For example, during two test deployments radio communication repeatedly failed to work inside the surveillance van.

---

[324] See Section 4.7.2.

[325] Match seven, 18th December 2018, Table 4.7.

[326] For example, match four, first Romford test deployment, 31st January 2019, Table 4.9. Another relevant point here is the way in which non-concluded searches are logged. After attempts were made to dispatch intercept this individual, discussion continued in the control room regarding the veracity of this match. After the subject could not be located it was decided (probably correctly) that this was unlikely to have been a verified match following an identity check. For the purposes of this report, this constituted an attempted intervention and is therefore recorded as such.

[327] Bethan Davies, Martin Innes and Andrew Dawson (2018) *An Evaluation of South Wales Police's Use of Automated Facial Recognition*, Cardiff: Universities' Police Science Institute, Crime and Security Research Institute, Cardiff University.

One example of how this effect played out in practice is alert four on 17th December 2018.[328] Here, when responding to a LFR alert, an adjudicating officer attempted to radio through a description of a matched individual. Responding to a failure of both the radio and the tablets and, crucially, a now shorter time in which to make an intervention, he elected to pursue the individual on foot. This led to an intervention with the individual and was resolved as a verified incorrect match. With longer reflection time after the event, a subsequent review revealed some important differences between the probe and gallery images.

Overall, technical difficulties therefore not only reduce the capability of LFR, they also compress the already limited time available for discretionary adjudication. Incidents such as this demonstrate the role of developing an environment that provides the most time possible for meaningful human adjudication in order to further mitigate the impact of incorrect matches.

4.8.2. Spatial Characteristics

The physical characteristics of a particular area, along with the spatial location of intervening officers, had significant bearing on the adjudication process and subsequent street intervention.

For example, during the Stratford test deployments officers were stationed very near to the cameras, situated either directly beneath them or a few metres behind, and therefore very close to the cameras' zone of recognition. However, this physical proximity compressed the time available for intelligence teams to exercise discretionary judgement when adjudicating LFR matches: within a few seconds of an alert being triggered by the LFR automated system, any matched individual would already be walking past officers responsible for intercepting them. So, the spatial deployment of officers that provided the best opportunity to locate a matched individual on the street, but at the same time significantly constricts the time available to adjudicators to reach a decision. Conversely, if officers are situated further from cameras, this affords more time for control room adjudication but increases the likelihood of losing track of individuals.

Another related element concerns the way space is organised *behind* the zone of recognition and how officers are located in relation to it. Related difficulties were particularly encountered at both the Stratford and Soho test deployments due to the complex crowd dynamics in the spaces behind the cameras. On several occasions, once an individual had passed a camera, and triggered an alert deemed credible, street-based intervention teams encountered difficulties in locating the matched individual. This suggests LFR technology has greater utility in certain specific types of spaces than others.

[328] Table 4.7.

Overall, spatial characteristics of the area under surveillance and choices about the spatial deployment of cameras and intervention team officers significantly influence the ability of officers to exercise discretion and adjudicate computer-suggested matches. While costs and benefits are associated with all decisions relating to the placement of intervention teams in relation to cameras, primacy should be afforded to the rights of citizens over operational convenience. The London LFR test deployments revealed that most computer generated matches were verified as incorrect.[329] In addition, police were more likely respond to an LFR alert with an attempt to intercept a matched individual.[330] This would suggest the importance of prioritizing spatial and temporal arrangements that maximise the possibilities for effective adjudication and discretion over factors easing the interception of matched individuals.

4.8.3. Operational settings

Less tangible, but potentially significant, are more ergonomic features of the operational environment, particularly those related to the amount of activity experienced by LFR operators. Alerts are not generated evenly throughout a given day. Over the course of the test deployments temporal clusters were discernible in the distribution of LFR alerts. At one end of the spectrum, and on several occasions, this led to intelligence teams having to deal with more than one alert at the same time. At the other end of the spectrum there are long periods of inactivity. Other ethnographic studies of video surveillance operations have identified the presence and influence of ennui in surveillance operation environments.[331] While this report focuses on trained law enforcement professionals, and does not question the ability of officers to act professionally when called into action, it is important to recognise how the atmosphere of operational environments changes when an alert is triggered. This was particularly apparent at the second Stratford trial where one sole alert was generated during a 10-hour deployment. Under these circumstances the alert rapidly transformed a setting of boredom to one of activity. This led to an intervention that resolved with an incorrect match. In future it could be useful to measure the tendency to adjudicate a computer-generated match as credible and decision to intervene, and the accuracy of decisions, following long periods of inactivity.

4.9. Engagement and resolving interventions

The test deployments revealed the important implications of how street-based engagements with matched individuals are resolved. This issue holds particular

[329] based on the calculation that 14 of 22 identify checks confirmed the LFR generated match was incorrect (see section 4.1.).

[330] 26 of 42 matches eligible for analysis. As noted above, the LFR technology generated 46 alerts over the observed trial deployments. Three alerts are discounted from the analysis here, having occurred before intervention teams were deployed, and another alert concerned an individual previously matched to the watchlist the same day. Hence 42 matches are counted as 'eligible' for analysis.

[331] Norris, C., and Armstrong, G. (1999) *The Maximum Surveillance Society*, Oxford: Berg; McCahill, M. (2002) *The Surveillance Web: The rise of visual surveillance in an English city*, Cullompton: Willan.

significance in relation to the rights of citizens, public acceptance of the technology, and public confidence in policing.

During the test deployments almost all LFR alerts led to one of two decisions: either a decision to engage with an individual based on an assessment of a credible match, or a judgment that a match was not credible. As the alert data shows, most computer-generated matches were deemed credible (26 of 42 matches eligible for analysis). One issue raised early on in the test deployments concerned the range of possible alternative responses to a computer-generated match while adjudication was occurring. This could include non-intrusive monitoring in place of engaging with an individual while adjudication was taking place.

Issues around interventions, and the implications for matched individuals, are illustrated by events following a number of verified incorrect LFR matches**.** As reported by civil society groups and national media, during the first Stratford trial an individual was matched by the LFR system and adjudicated as credible by the intelligence team, launching a decision to conduct an identity check. Yet this individual had already been subjected to a 'stop and account' minutes before by different officers due to his behavioural response to a nearby knife arch,[332] and considered innocent of any wrongdoing. Following a LFR-initiated match, and confirmation of its credibility by adjudicating operators, minutes later the individual had to produce identification for the second time (this was a verified incorrect match).

Police stops of matched individuals have also led to criticism from civil society groups about the heavy-handed nature of some of these interventions. Particular criticism has been raised about one of the Romford test deployments where a 14-year-old child was questioned by police. This occurred when street-based intervention teams responded independently to an LFR alert transmitted to their handheld devices. This alert was later adjudicated by intelligence teams in the control room as non-credible, although at this point the intervention had already been made. One of the researchers witnessed this stop at close quarters and has since reviewed video footage of the episode.[333] Here, a uniformed schoolboy was stopped and surrounded by five plainclothes officers around 20 metres from the van, and led by the wrists to a side street. He was visibly distressed and clearly intimidated. An identity check resulting in a verified incorrect match was followed by conflict on the streets with an adult female shouting at the officers and complaining about the police engaging with children in this manner.

[332] An operation being conducted quite separately from the LFR test deployment but in the same location.
[333] Alert 14, 14th February 2019, table 4.10.

After reviewing video footage, and speaking with the boy's mother, Silkie Carlo, Director of Big Brother Watch, describes the implications as follows:

> It's probably important to report [the case of] a 14 year old boy who was misidentified and stopped and searched on the last day of the Romford deployment. I've seen the footage of it and … spoken to his mum about it, who's furious, … Naturally, the child now has formed a completely negative view of the police and what he looks like to adults in general and police officers. I can't imagine how terrified I would be if four plain-clothed men appeared out of the blue and dragged me off by my wrists to one side, let alone as a 14 year old child, and this is a gateway technology that allows police to conduct stop and search with the veil of this kind of objectivity of facial recognition cameras.

This incident brings together a number of problematic aspects of LFR deployment, starting with the problem of on the street officers not waiting for control room adjudication – a clear example of the presumption in favour of intervention. It is also an all too vivid illustration of the LFR technology's potential for 'surveillance creep', as indicated in the quote above. Last but not least, this illustrates difficulties surrounding how LFR alerts are resolved through engagements with the public, particularly when it involves the police handling of young people.

In remarks articulated after the test deployment senior officers involved appeared well informed over the implications of such incidents and recognised the need to address this the means of engaging with matched subjects in future test deployments. One of the issues at stake here appears to be the different types of police specialism and the disparities of hierarchy involved in such operations. More than one senior officer pointed to the (organisational) cultural difficulties surrounding those in senior ranks telling uniformed officers how they should act in street-based settings.

Ends

The Human Rights, Big Data and Technology Project

Human Rights Centre,
University of Essex,
Colchester CO4 3SQ
+44 (0)1206 872877

@HRBDTNews
www.hrbdt.ac.uk