LONDON POLICING ETHICS PANEL

FINAL REPORT ON LIVE FACIAL RECOGNITION

MAY 2019

The ‘London Policing Ethics Panel’ (LPEP) is an independent panel set up by the Mayor of London to provide ethical advice on policing issues that may impact on public confidence.

LPEP complements the existing structures in place in the capital to oversee the way London is policed, and provides in-depth consideration of ethical issues around current and future policing practice in London.

CONTENTS

EXECUTIVE SUMMARY

Facial recognition technology is one of a potentially larger set of tools associated with the deployment of new digital technologies in policing contexts. Since 2016 the Metropolitan Police Service (MPS), along with other police services, has been trialling a specific form of Live Facial Recognition (LFR). These trials have attracted attention from press and public, raising important questions about the power of new digital technologies, how they are tested in the field, and their potential to impact on the relationship between police and civil society.

This Report builds upon our earlier Interim Report. Here we:

- report the views of Londoners on use of Live Facial Recognition, as gathered through our survey;
- propose an ethical framework to adopt in future police technology trials;
- set out conditions the Panel views as reasonable to attach to adoption of LFR in policing operations;
- share an ethical thought-experiment exploring the implications of increased police surveillance.

What is special about Live Facial Recognition?

Live facial recognition enables the police to conduct identity checks assisted by an automated recognition system, in real time and in public places. Facial features are scanned as people pass by cameras utilising specialised software. These are automatically checked against facial images on a 'watch list'. These are images drawn from custody photographs and other police sources.
During the LFR trials, the images used were of people wanted by the police for specific offences or because they posed a risk of violence to others. The LFR technology flags potential matches to a nominated police officer, who assesses the alert.

Developments in the past decade have demonstrated how digital technologies can significantly impact on relationships of trust in social, commercial and political spheres. We can expect digital technologies to have similar impact on trust in policing. A concern to understand, preserve and build trust in policing is therefore apparent throughout our report.

Since we started our work on LFR the Home Office has published its Biometrics Strategy.[1] The Home Office Biometrics and Forensics Ethics Group (BFEG) published a briefing on LFR in December 2018.[2] Additionally, in March 2019 the Surveillance Camera Commissioner published guidance to assist policing authorities using LFR to comply with their statutory obligations arising from Section 31(1) Protection of Freedoms Act 2012 and the Surveillance Camera Code of Practice.[3] We refer to these where appropriate.

We are conscious that we are preparing this report without recourse to the LFR trial data or the independent evaluation commissioned by MPS. We therefore do not express a view on whether LFR has yet been shown to be a fair, efficient and effective use of police resources.

1. https://www.gov.uk/government/publications/home-office-biometrics-strategy
2. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/781745/Facial_Recognition_Briefing_BFEG_February_2019.pdf
3. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/786392/AFR_police_guidance_of_PoFA_V1_March_2019.pdf

What do Londoners think about police use of LFR?

We start by considering public views on live facial recognition. We do not believe public opinion can determine what is ethically acceptable or morally right in any straightforward way. Majority opinion does not justify morally questionable actions, and the views and interests of minorities deserve protection. However, the process of eliciting and seeking to understand Londoner's views on how their city ought to be policed is an important ethical task. It indicates how using LFR might impact on trust, how London's different communities might view LFR, and how far the public view using LFR as a proportionate response to different policing problems.

A weighted sample of 1,092 Londoners responded to our survey, and a sub-set of 50 respondents was invited to take part in a follow-up telephone interview. All were given a description of how LFR worked, based on the technology used in the trials.

The purpose for which LFR might be used makes a significant difference to people's support. In general terms, more than half of our respondents thought that police use of LFR could be acceptable. However, views on using it to identify people wanted by the police vary considerably according to the seriousness of the crime. In the case of serious crimes, support varied between 83-81% depending on the nature of the threat; for minor crimes it falls to 55%, and below 50% for dealing with nuisance behaviour.

Half of respondents thought using LFR would make them feel safer. A little over a third also worried about its impact on their privacy, and were concerned that police would be collecting data on people who had not committed a crime. Almost half of respondents thought the technology would lead to personal information being collected more often about some groups than others. Younger people were less accepting of police use of LFR than older people, and people from Asian and Black ethnic groups were less accepting than those from White groups.

We also asked survey participants whether they would be likely to stay away from events where LFR would be in use (a so-called 'chilling effect'). Overall fewer than one in five respondents thought that they might stay away from events, but there was significant variation across socio-demographic variables. Younger people were much more likely to say they would stay away from LFR monitored events – 38% of 16-24 year olds compared to 10% of those aged 55 and over – as were people from Asian, Black and Mixed ethnic groups.

Additionally, it should be noted that in our interviews some commented that they would be more likely to attend LFR monitored events, as they would feel safer.

Of note given the potential growth in data driven policing, only 56% of those we surveyed thought that police would use their personal data in accordance with the law.

Trust formed an important lens through which participants in the survey viewed LFR. Those who had high levels of trust in the police in general were much more supportive of using LFR, perhaps because they thought the police would use the technology and their data appropriately to make policing more efficient and effective.

It seems likely that trust will also form the prism through which people view future police technology developments. Research on public acceptance of new technologies regularly finds higher levels of acceptance among people who trust those (such as scientists) using the technologies. For this reason it would seem prudent to ensure that steps are taken now to build and maintain the public's trust in police use of new technologies, for example through robust governance of field trials, and meaningful controls over deployment. This may mean imposing self-limiting constraints in order to be able to reap the benefits of supportive technologies. Trust once diminished is hard to rebuild.

How should new policing technologies be trialled in future?

Field trials of policing technologies present distinctive ethical challenges, because they are a hybrid of research and policing operation. We recognise that the ethical precepts governing field research and governing policing activity in some respects conflict, particularly over what may constitute legitimate grounds for coercion. We believe there is a need for good field trials of policing technology, and have therefore proposed a framework to support analysis of the ethical issues they raise.

We suggest that key components of an ethical policing technology field trial are robust trial design addressing questions both about the technology's capability and how it will function in varied policing uses; and adherence to principles that protect citizens from risk and harm. Our proposed ethical framework invites those planning a trial or introducing new technology to consider how it will impact on individuals, specific groups (such as vulnerable people or particular communities) and society in general.

Our framework groups fourteen principles into four overarching domains, with suggested questions providing guidance on applying each of the principles:

Domain One - serving the public

- Policing technology trials adopt principles of openness, inclusivity and engagement, and strive to maintain trust in policing.

Domain Two - robust trial design

- Policing technology trials are purposeful and well-designed, potential risks and benefits to participants have been weighed, and the design and operation of trials are underpinned by the necessary expertise and judgement.

Domain Three - respect for equality, dignity and human rights

- Policing technology trials respect diversity, technologies are tested to be free from bias, participation in a trial is not coerced or invasive, and any interference in individuals' rights is proportionate.

Domain Four - addressing concerns and outcomes

- Ongoing policing technology trials are subject to continuing ethical appraisal, responsive to emerging concerns, and provide for rectification of wrongs if they arise.

ETHICAL CONSIDERATIONS AND PROPOSED CONDITIONS FOR USING LFR

Assuming the MPS trials demonstrate LFR offers significant operational benefits, we have come to the view that there are important ethical issues to be addressed but these do not amount to reasons not to use LFR at all. We argue therefore that MPS should proceed with caution and ensure that robust internal governance arrangements are in place that will provide sound justifications for every LFR deployment.

We concur with the views of several others, including the BFEG and Surveillance Camera Commissioner, in respect of the ethical issues to be taken into account. We comment briefly on the ethical implications of current legal protections. Further ethical concerns are grouped under two headings: injustices associated with misidentification, and potential incursions on civil liberty.

Current legal protections

Following our Interim Report, the MPS made public its own analysis of the legality of its use of LFR and we do not challenge this legal analysis. Some of our ethical concerns regarding use of LFR are akin to those arising in respect of all forms of police surveillance, which are partially addressed by Article 8 of the European Convention on Human Rights. This requires any interference with privacy rights to be in accordance with law, and necessary in a democratic society in furtherance of legitimate aims.

The Surveillance Camera Commissioner has provided further guidance on the law and notes the protections to be afforded to other human rights including freedom of assembly, freedom of thought belief and religion, freedom of expression, freedom of association, and protection from discrimination in the exercise of those rights.

The fundamental rights, freedoms and protections enshrined in the ECHR set a legal threshold for deploying LFR. They also highlight some of the ethical concerns associated with its use.

Injustices associated with misidentification

Concerns have been raised by both scientific and civic groups regarding possible intrinsic biases in LFR technology, which may mean it is less effective at identifying BAME and female faces. This bias might in turn permeate policing operations in which the technology is used. Whether and how bias would emerge depends on the nature of the policing operations in which LFR is used, how police personnel interact with the technology when it is used to assist identification, and how the police respond in field situations.

We suggest that MPS trial data are potentially a source of insight into any intrinsic bias, and should help to indicate how such bias would or would not feed forward into policing operations. We argue it is in the public interest to publish the trial data and evaluations, to address these concerns. Additionally, because the actions of human operators affect the technology's functioning in the field and therefore the public's experience of automated recognition, appropriate LFR operating procedures and practices need to be developed.

We note that while the technology may be imperfect, so too is human recognition capability and we think it would be useful to include it as a baseline in all identification technology assessments.

Potential incursions on civil liberty

We consider necessity, proportionality and policing by consent; the integrity of the databases from which the watch list is compiled; and the potential 'chilling effect' of police surveillance.

We concur with the BFEG and Surveillance Camera Commissioner that deployment of LFR must observe principles of necessity and proportionality. Neither of these principles could be satisfied by unrestricted use of LFR.

Proportionality is a matter of judgement and we believe this is where understanding the opinions of Londoners can be of value. As we note earlier, public opinion cannot be treated as definitive. However, we believe that it gives an indication of how members of the public gauge proportionality, and the extent to which there would be a generalised social consent to police use of LFR. Broadly, the more serious the crime or threat the more clearly proportionate use of LFR is seen to be; and the less serious the crime or threat the less its use appears proportionate and consistent with the principle of policing by consent.

This suggests that LFR deployments should be limited to managing more serious offences. This in turn has significance for compilation of the LFR watch lists, which should only include images from people wanted for serious offences or presenting serious threat of harm.

During the LFR trials, most images were drawn from the MPS custody databases, but some were also drawn from other sources available to the MPS. We have drawn attention to concerns regarding the databases (or other sources) from which images are selected. Images must be from a legitimate source and up to date, so that persons on the watch list are still wanted for serious offences at the time of deployment.

We respect the arguments that a range of commentators have made, drawing attention to the possible negative effects on society of increased police surveillance through LFR.

A central objection is that surveillance has the potential to produce a chilling effect on democratic debate and protest, and more generally dissuade people from engaging in legitimate activities in public space. We have given consideration to this argument, and the counter-argument that surveillance can make public spaces safer, including for vulnerable groups. Both arguments rest on predictions about how surveillance technologies might be used or potentially abused, views on the value accorded to liberty and to safety, and levels of trust in policing. The interests represented on both sides are important ones.

The Panel's view is that if it is shown there are significant legitimate policing benefits to be gained from LFR these should nevertheless not be gained at the expense of valued liberties. Given the framework of legal obligations that currently exists, we propose that an appropriate ethical response is to implement robust internal governance procedures that ensure police uses of LFR technology meet, and to some extent surpass, these legal obligations.

PROPOSED CONDITIONS

In summary, LFR should only be deployed where the following five conditions can be met.

1. It can be shown that the use of LFR offers more than marginal benefit to the public, sufficient to compensate for the potential distrust it may invoke.

2. It can be shown from trial data (and other available data) that the technology itself will not import unacceptable gender and racial bias into policing operations.

3. Controls on use are sufficiently robust to ensure that each LFR deployment is appropriately assessed and authorised, when it is judged both necessary and proportionate to use it for a specific policing purpose.

4. It can be shown that human operators will be knowledgeable about the potential injustices that may be caused by an inappropriate response to identification alerts, that they know how to avoid these, and are accountable for their actions.

5. MPS and MOPAC develop robust governance and oversight arrangements that balance the technological benefits of LFR with their potential intrusiveness. These should meet the Home Office Biometrics Strategy's requirement for transparency, take into account guidance from the Surveillance Camera and Biometric Commissioners, and compensate for the limited powers of the Surveillance Camera Commissioner to inspect, audit or enforce compliance.

   Such provision would include:

   a. operating procedures that govern the compilation of LFR watch lists, including provision for ensuring that data are accurate, current, and limited to the agreed policing purpose for the deployment;

   b. operating procedures that govern authorisation and deployment of LFR ensuring its use is legal, necessary, and proportionate on each occasion;

   c. provisions for transparency regarding LFR deployments, for example through publishing data in respect of LFR deployments on MPS's public facing statistics and data dashboards;

   d. oversight by MOPAC in a manner akin to MOPAC's oversight of other potentially intrusive tactics.

Additional recommendations

We are also making three recommendations.

i. We recommend that when designing and conducting future trials of new policing tools and technologies, MPS incorporates consideration of the ethical framework that we propose in this report into its planning processes.

ii. We recommend that in the event MPS proceeds to adopt LFR, approximately 12 months after the first LFR deployment MOPAC should gauge its effects through incorporating elements of the public opinion survey carried out for this report into MOPAC's next quarterly Public Attitudes Survey.

iii. Anticipating future technological developments, MOPAC and MPS should continue to draw Home Office attention to the need to simplify and strengthen the regulation of new identification technologies.

Afterword: a thought experiment

We are living in an information age when new digital technologies may be able to offer real value in achieving fair, effective and efficient policing in a global city. As with LFR, some of the benefits of new technologies will also bring with them anxieties about how we protect our liberties now and in the future.

In the final section of the report we offer a thought experiment with the aim of contributing to further public debate about how to respond to the promise and perils of potentially ever more intrusive technologies. These are not just technical questions, but questions about our values, how we see policing fulfilling its obligations to all of London's different groups and communities, and about what we most cherish in our social arrangements.

TERMINOLOGY

This report adopts the terminology and definitions used by the BFEG and based on the International Standards Organisations (ISO) biometric vocabulary (ISO 2382-37).

- *Biometric recognition* is the automated recognition of individuals based on their biological and behavioural characteristics, for example, facial image, DNA, voice and gait.
- *Automated recognition* implies that a machine-based system is used for the recognition, either for the entire process or assisted by a human being.
- *Live facial recognition* (LFR) is the automated one-to–many 'matching' of near real time video images of individuals with a curated 'watch list' of facial images

The Surveillance Camera Commissioner uses the broader term Automated Facial Recognition.

1. INTRODUCTION

Facial recognition technology is one of a potentially larger set of tools associated with the deployment of new digital technologies in policing contexts. Since 2016 the Metropolitan Police Service (MPS), along with other police services, has been trialling a specific form of Live Facial Recognition (LFR).

These trials have attracted attention from press and public, raising important questions about the power of new digital technologies, how they are tested in the field and their potential to impact on the relationship between police and civil society.

The London Policing Ethics Panel issued an Interim Report in respect of the MPS LFR trials in July 2018, making recommendations that aimed to enhance the trials and their governance. The MPS responded to our recommendations, and continued to test the technology in further field trials completed in February 2019.

This Final Report builds upon our Interim Report. Here we:

- describe the type of facial recognition technology that was trialled in London
- report the views of Londoners on use of Live Facial Recognition, as gathered through our survey and interviews;
- reflect on the ethical lessons that can be learned from the field trial process, and propose an ethical framework to adopt in future police technology trials;
- set out conditions the Panel views as reasonable to attach to adoption of LFR in policing operations;
- share an ethical thought experiment exploring the implications of increased police surveillance.

The Metropolitan Police Service shared information with the Ethics Panel about its current technology, responded to the recommendations we made in our Interim Report, and invited us to observe and comment upon its field trials. We are appreciative of the MPS's engagement with the Panel during our consideration of LFR, and its responsiveness to the questions we have raised. In the latter stages of our work we have been able to draw on the Home Office Biometrics Strategy,[4] the briefing published by the Biometrics and Forensics Ethics Group,[5] and the guidance published by the Surveillance Camera Commissioner.[6]

We are conscious that we are preparing this report without recourse to the LFR trial data or the independent evaluation commissioned by MPS. We therefore do not express a view on whether LFR has yet been shown to be a fair, efficient and effective use of police resources.

What is special about Live FR?

This document discusses the Live Facial Recognition technology (LFR) that has been the subject of public trials by the MPS. The term Automated Facial Recognition (AFR) is often used by commentators, but bears a wider meaning. Simple automatic facial recognition is increasingly familiar to consumers through applications such as facial 'tagging' on social media and use of facial recognition for logging on to electronic devices. More sophisticated forms include advanced video analytics that can be used to review recorded media. None of these forms of facial recognition facilitate identity checks in public places in real time. This is the process specific to Live Facial Recognition.

As trialled, LFR is an assistive recognition technology that predicts the probability of a match between a live captured image and an image on a watch list. LFR enables the police to conduct identity checks in public places in real time, supported by an automated system. The police could potentially also co-operate with private bodies (for example retail consortia) that might use the same assistive technology to carry out identity checks in private places in real time.

The public is already accustomed to the widespread use of closed circuit video recording (CCTV) in both public and private spaces. CCTV records images of people and activities with varying degrees of precision and efficiency, and requires substantial human input to identify individuals. The public is also accustomed to the use of automated number plate recognition (ANPR). ANPR automatically captures information, with a reasonably high degree of accuracy, regarding the movement of vehicles. These vehicles are in turn traceable to their owners, although this will not necessarily identify who was the driver at the time.

However, while LFR has some features in common with both CCTV and ANPR it is in other respects quite different. Like CCTV it can be used to identify individuals of interest, and like ANPR it can be used to capture information automatically from recognisable features. But by comparison with CCTV, LFR is potentially more far reaching because it partially automates the process of identifying and tracking individuals through their facial features. And use of LFR raises questions that ANPR does not, because LFR is not identifying disposable and transferable objects registered to owners but more or less permanent identifying characteristics of individuals. No one is obliged to own a car, but we all possess a unique face.

Finally, we recognise that commercial and consumer applications of facial technology are growing exponentially and are in many instances welcomed by the public. However, the use of LFR in policing presents different and important questions about its effects when it is used in combination with police powers. As the Home Office Biometrics Strategy notes, biometric technologies have different implications in different contexts. Where used by public authorities, important considerations will be the necessity and proportionality of a given use, potential risks to privacy, and the robustness of the techniques used to collect and process biometric data. They propose that as well as their use being lawful there should be "a presumption of transparency", a conclusion with which we strongly agree.[7]

The form of LFR that has been trialled

In the trials undertaken by the Metropolitan Police Service, the LFR under testing was of a quite limited form.

At each trial, fixed cameras with utilising software were set up at a specific location to scan the faces of people walking past the camera. To assess facial identity people have to be channelled past the camera(s), and environmental conditions such as light and camera angle come into play. In Live Facial Recognition facial images are scanned only for as long as is necessary for real time analysis. Images that generate an alert are retained while images that do not generate an alert are immediately discarded.[8]

As facial features are scanned they are automatically checked against facial images on a watch-list. During the trials a bespoke watch list was created specifically for each deployment of the technology, drawing from the Metropolitan Police Service's databases of photographs. The majority of photographs used to compile the watch list were those taken when a suspect was in custody, but other police sources were also used.

The LFR technology flags potential matches to a nominated police officer, who conducts a visual check and assesses the alert. If the officer holds a reasonable belief in the credibility of the match, and judges that an intervention is warranted, action may then be taken.

The MPS emphasised that no action would be taken until after at least one police officer had visually assessed the accuracy of the match. In some operations, one operator may assess the initial alert while an officer on the ground will receive information regarding a possible match. The officer on the ground will then make the operational decision whether to intervene, for instance, whether to enter a crowd to engage with the person concerned. Hence LFR technology was being used to support police recognition activity, rather than functioning as a pure automated recognition system. The MPS completed a total of ten LFR trials before concluding the field trial stage of evaluation.

The Panel's approach

The use of LFR technology is in its infancy in UK policing. There are currently significant limitations in terms of how and where LFR might be used, and therefore the types of outcomes it might produce. But it is a defining characteristic of new technologies that their eventual reach is unpredictable, a characteristic which makes ethical assessment particularly challenging. We sought to be realistic in our ethical assessment by grounding it in LFR's current capabilities, whilst also being attentive to the benefits and harms associated with a more highly developed version of the technology. Overestimating future benefits and harms "may well lead to a focus on scenarios that are morally thrilling but very unlikely" (Van de Poel, 2016) but some degree of ethical imagination is imperative. When novel technology is introduced it is relatively uncontrolled and its uses experimental, so it is hard to gauge its impact. By the time a technology is more established, it may be too difficult to halt its use irrespective of harms or negative effects. (Collingridge, 1982)

This report is shaped by the need to grapple both with what we know about the novel technology of Live Facial Recognition, and also with what we do not yet know about how it - and similar novel policing technologies - might work.

We have taken into account three levels at which policing technologies could have an impact. The first 'micro' level is individuals, who may experience effects (such as moral, legal or physical harms and benefits) specific to themselves and their close associates. At the next level up, the 'meso' level, policing technologies may impact in different ways on particular communities, social groups, sub-populations, or organisations.

London's extraordinary diversity, in terms of gender, sexuality, age, ethnic group, country of birth, socio-economic class and so on, is both a fact and a precious asset. We have therefore endeavoured to be attentive to how policing technologies may affect some communities more than others. Finally, at a 'macro' level, there is a need to consider the effects of policing technologies on society and its institutions as a whole, over time.

The underlying principle guiding the Panel's work is that ethical policing in a global city rests on a sound and enduring relationship of trust between the police service and those who live in, work in, or visit the city. Trust is at issue when we rely on others to carry out responsibilities that we ourselves cannot perform. It entails a willingness to be vulnerable to the power of others, notably when someone, some thing or some outcome that we value (such as personal safety) is at risk in some way. When we place our trust in people and organisations we expect they will be competent and act with good intentions. This trust is the foundation on which policing rests, enabling it to fulfil its purposes of protecting the public, maintaining individual freedoms, and serving justice.

Developments in the past decade – for example digital commerce and the rise of cyber crime, the connectivity promoted by social media and the rise of 'fake news' - have demonstrated how digital technologies can significantly impact on relationships of trust in social, commercial and political spheres. We can expect digital technologies to have similar impact on trust in policing. A concern to understand, preserve and build trust in policing will therefore be apparent throughout our analysis.

4. https://www.gov.uk/government/publications/home-office-biometrics-strategy

5. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/781745/Facial_Recognition_Briefing_BFEG_February_2019.pdf

6. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/786392/AFR_police_guidance_of_PoFA_V1_March_2019.pdf

7. Home Office Biometrics Strategy para.

8. During the trials, a video recording was made of people passing by the camera in order to support technical analysis of the trial data. This recording was retained for 30 days, whilst the technical assessment was carried out, and then deleted. No images were extracted from this video.

2. WHAT DO LONDONERS THINK ABOUT POLICE USE OF LFR?

We start by considering public views on Live Facial Recognition. We should be clear that we do not believe public opinion can determine what is ethically acceptable or morally right in any straightforward way. However, the process of eliciting and seeking to understand Londoner's views on how their city ought to be policed is an important ethical task for several reasons.

First, as trust is the foundation on which good policing rests we used our survey to explore how trust in the MPS may be affected by LFR. We asked people to weigh the policing outcomes they valued against their vulnerability to the additional power this new technology may grant the police.

Second, we have endeavoured to take into account three levels at which policing technologies could have an impact: individuals, specific communities, and larger society. We used our survey to understand how people thought LFR might impact on them individually, and how it they thought it might impact on different communities.

Third, proportionality is an important legitimising principle for the exercise of police power. (Broadly speaking, proportionality requires that use of police powers does not go beyond what is required to pursue legitimate goals.) Proportionality is not an objective measure, but one that rests on continuing negotiation of different perspectives leading to some degree of social consensus. We have tested in our survey the policing outcomes people most value, how far they feel their freedoms would be curtailed if police had recourse to LFR, and what sort of police uses of LFR might be justifiable. This gives us some insight into how Londoners might judge proportionality, and therefore the extent to which using LFR can be viewed as consistent with policing by consent.

Method and sample

On behalf of the London Policing Ethics Panel, MOPAC and the UCL Institute for Global City Policing commissioned Opinion Research Services (ORS) to conduct a survey capturing Londoners' views on Live Facial Recognition (LFR), along with more general perceptions on police use of personal data. Respondents were identified using YouGov's Omnibus: a UK panel of 800,000+ individuals who have agreed to take part in surveys. Panellists received an e-mail inviting them to take part in the survey. A total of 1,092 Londoners responded to the survey between 23 May and 4 June 2018.

The responding sample was weighted to provide a representative sample of the London adult population (aged 16+).

In addition to the survey, a sub-set of respondents was invited to take part in a follow-up telephone interview. The interview was designed to further explore themes that emerged from the survey, including people's 'thresholds' for appropriate uses of LFR, whether the presence of LFR would deter them from going to a public event, and wider views regarding trust in police and accountability. A total of 50 people were interviewed including 29 males and 21 females. The majority of interview respondents were White (n=36), 10 were Asian, and the remainder were Black or of Mixed ethnic origin. Most of the interviews lasted for around 15 minutes and were undertaken by ORS's qualitative research team. Interviewees were assured of complete confidentiality and that they were free to be as open and honest as they wished insofar as they would not be named in the report.

We have used the acronym LFR in this report. However, the acronym AFR was used when commissioning the survey. To avoid confusion, we have referred to LFR throughout. Respondents were provided with this description of how Live Facial Recognition works:

> "The technology involves the use of cameras at specific public events which scan the faces of those passing by and flag up potential matches against a 'watch-list' of images of individuals of interest to the police (e.g. those with an outstanding arrest warrant). Only images that come up as a match on the watch-list are retained by police; images of people not on the list are immediately discarded".[9]

Overall views on LFR

Overall 57% of respondents thought that in general terms, police use of LFR was acceptable. We will see, however, that the purposes for which it is used makes a significant difference to people's support for its deployment.

Table 1 presents acceptability of LFR by socio-demographic characteristics. There was little significant variation in views by gender, country of birth, social class, or victimisation experience. By contrast, younger people were less accepting of police use of LFR than older people, and people from Asian and Black ethnic groups were less accepting than those from White groups.

We also asked respondents more specific questions about their views on police use of LFR. As **Figure 1** shows, although the Londoners in our survey were positive about the possibility of LFR assisting police to catch criminals (three-quarters felt this), they were more divided on whether it made them personally feel safer, with views on this question split 50:50.

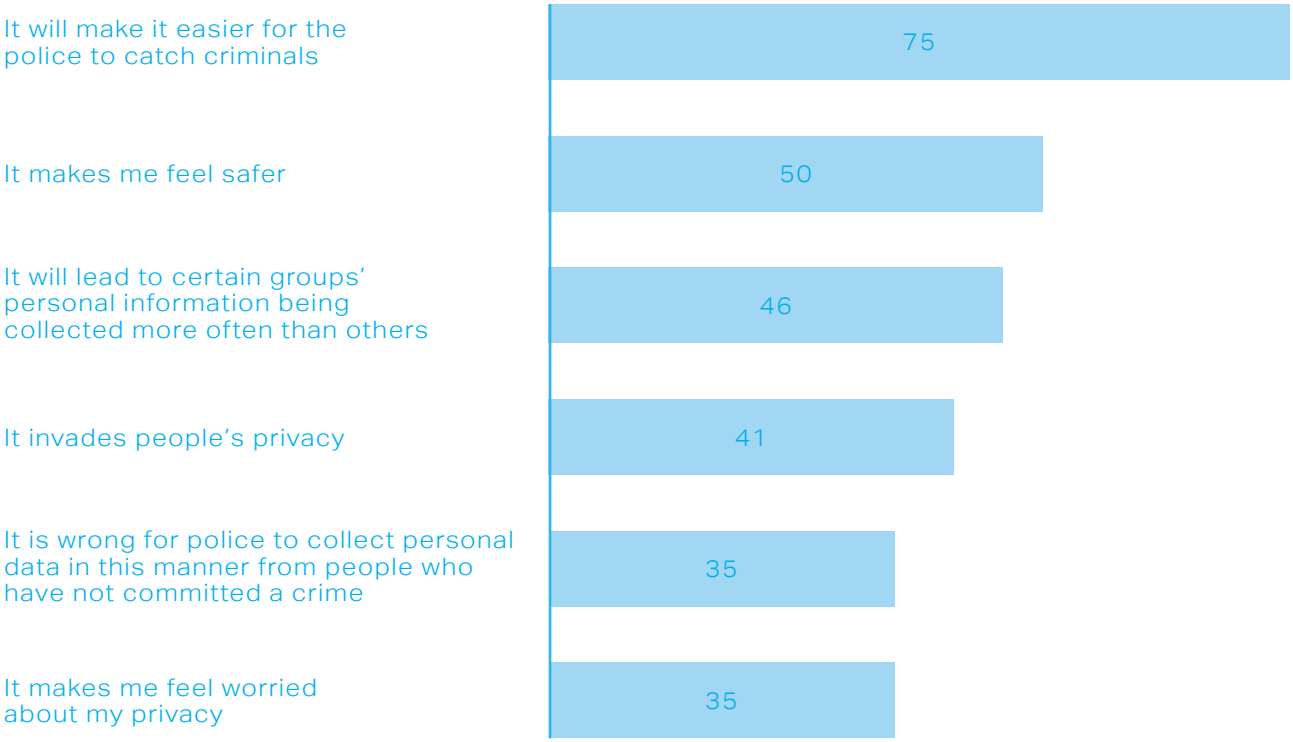
TABLE 1: DO YOU THINK IT IS ACCEPTABLE OR UNACCEPTABLE FOR THE MET POLICE TO USE LFR?

		% agree	n
Gender	Female	57	552
	Male	57	540
Age	16-24	45	147
	25-39	48	341
	40-54	62	301
	55+	66	303
Ethnic group	Asian	44	233
	Black	37	44
	Mixed	65	48
	White	63	698
Country of birth	UK	58	852
	Outside UK	55	213
Social class	ABC1	57	644
	C2DE	57	449
Recent victim of crime	No	56	896
	Yes	60	167
Total		57	1093

Note: Percentages calculated with missing values excluded
Weighted data

9. Note that the survey included a 'split-ballot' experiment, wherein some respondents received the accurate description of MPS use of LFR shown here. Others, however, received a slightly amended version, which replaced the last sentence with "These images, including those of people not of interest to the police at the time, could potentially be retained for use in future investigations, for example to reconstruct the movements of a person suspected of a crime". The aim was to explore whether respondents reacted differently to hearing that images were kept rather than discarded. However, there were no significant between the two conditions in, for example, measures of acceptability. We therefore present figures from a sample that combines these two conditions in this report.

FIGURE 1: PERCENTAGE AGREEING WITH SPECIFIC VIEWS ON LFR



What might Londoners consider to be reasonable use of LFR?

Although a majority - 57% - of respondents to our survey agreed police use of LFR was acceptable, degrees of acceptance depended on the specific purposes and setting in which the technology might be used. In the survey respondents were asked "In principle, to what extent do you agree or disagree it would be acceptable for the Metropolitan Police" to use LFR in train stations and at ticketed events at a major arena to:

- identify potential terrorists
- identify people wanted by the police for serious violent crimes
- identify people wanted by the police for minor crimes
- identify people wanted for nuisance behaviour

Reponses to the eight items are summarised in **Figure 2** which shows the proportion answering 'strongly agree' or 'somewhat agree' to each. Items are also ranked, from the use securing the highest level of agreement (LFR to scan crowds at train stations to identify potential terrorists, 83%) to the use securing the lowest agreement (LFR to scan crowds at train stations to identify people wanted for nuisance behaviour, 45%).

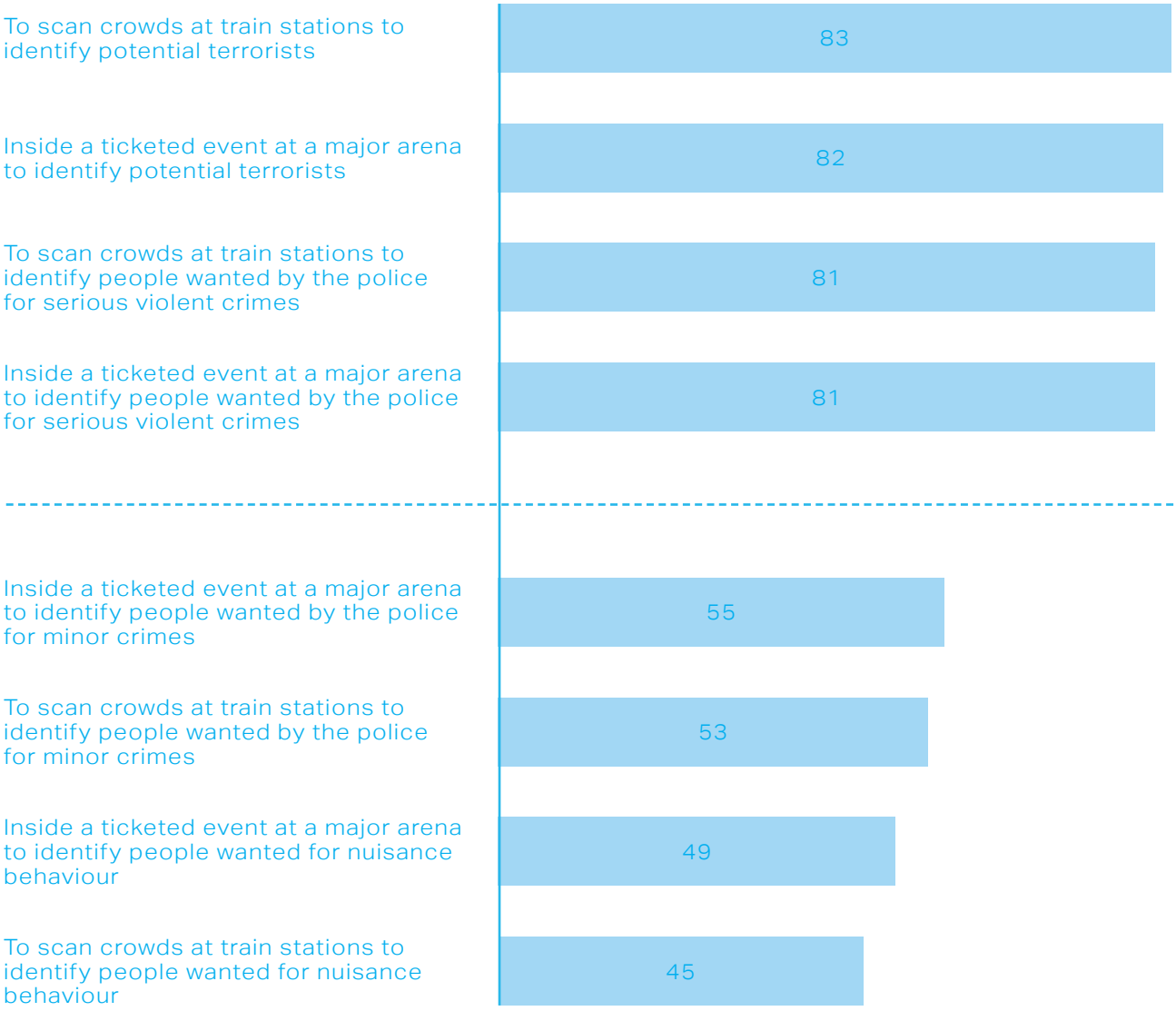
Two findings are of particular note. First, there is a clear rank order, with support for use to identify terrorists and those wanted for serious violence significantly higher than support for use to identify those wanted for minor crime and nuisance behaviour. Note also the 'break' in the figure between the least widely supported use in the serious offences category (LFR inside a ticketed event at a major arena to identify people wanted by the police for serious violent crimes, 81%) and the most widely supported use seen in the in the minor crime category (LFR inside a ticketed event at a major arena to identify people wanted by the police for minor crimes, 55%). Many respondents clearly felt it was appropriate to use LFR in the case of serious crimes but not in relation to less serious crimes.

Second, however, in only two cases (both relating to LFR use to identify people wanted for nuisance behaviour) did support fall below 50%. So, while respondents clearly did draw a strong distinction between various potential uses of LFR, they were in effect starting from a relatively high base line of acceptability, and, when told the technology was to be used to search for serious offenders, support was almost overwhelming.

When we interviewed a selection of respondents we explored their thinking further using two examples of possible deployments: (1) to deter people from going to places they should not be, for example where they have an exclusion order in place; and (2) to apprehend people who have committed a crime or are wanted by police. Views on using LFR to deter people from going to places were mixed. Some generally considered this to be a 'good idea', especially for situations where individuals had been banned from football matches, for example. Others were sceptical about this potential use of LFR and argued that LFR would not necessarily prevent people from going to places they should not be. There was also concern that knowing LFR was in use would 'scare away' people the police wanted to apprehend. It was felt there were more suitable ways to deal with these types of people (e.g. frontline policing) and that it should not be the primary use for LFR.

On the other hand, the idea of using LFR to apprehend criminals or people who are wanted by the police was well received, and the vast majority deemed it to be appropriate as long as 'people of interest' is clearly defined. Participants were hopeful the technology would allow police to make identifications more quickly and accurately than CCTV and human observation, which they felt would be especially helpful due to the service's apparent issues with cuts and lack of resourcing. Again, nearly everyone felt that using LFR for this reason would be acceptable at most public events, while some thought it would also be beneficial to monitor train stations and shopping malls. However, more widespread and intrusive use of the technology, for example on residential streets, was not considered appropriate.

FIGURE 2: PERCENTAGE AGREEING ON APPROPRIATE USES OF LFR



The majority of people who participated in the additional interviews thought LFR should be used in relation to all types of crime, although it was acknowledged that if time/resourcing did not permit this then serious crimes should be prioritised. We should note though, there was agreement that it would not be appropriate to use LFR for low-level offences such as unpaid parking fines, speeding offences and fly tipping. Some respondents argued that police officers on the beat should be dealing with less serious crimes and that using LFR for this purpose could be the thin edge of the wedge to London/the UK becoming a surveillance state.

Over one-third of those surveyed had concerns about LFR relating to privacy, both in relation to themselves and others, along with the ethics of police collecting data from people who have not committed a crime. Furthermore, almost half of respondents had concerns relating to how fair the use of the technology would be, with concerns that LFR might lead to certain groups' personal data being collected more often than others.

> ***"That would be an awful lot of cameras in a lot of places, and I don't think I would want to see them on every lamppost or in every car park."***

Could LFR have an adverse impact on London or some of its communities?

London is a vibrant and diverse city that hosts a vast array of political and cultural events, cultural practices, and counter-cultural activity. Its social and cultural dynamism is a precious characteristic, to be protected along with public safety, moral interests and human rights. An important question in relation to police use of LFR is whether state surveillance has a 'chilling' effect on social activity in public spaces, for example through deterring people from gathering at political or counter cultural events. Alternatively, might higher levels of surveillance have a 'warming' effect, allowing people who might otherwise feel excluded from public spaces to use them confident that they will be safe?

We asked survey participants how far they agreed with the statement "I would stay away from events where I know LFR would be used". While overall less than one in five respondents agreed that they might do this, there was significant variation across socio-demographic variables. **Table 2** shows that younger people were much more likely to say they would stay away from LFR monitored events – 38% of 16-24 year olds compared to 10% of those aged 55 and over – as were people from Asian, Black and Mixed ethnic groups.

TABLE 2: STAYING AWAY FROM LFR MONITORED EVENTS BY SOCIO-DEMOGRAPHIC CHARACTERISTICS

Agree with the statement: "I would stay away from events where I know LFR would be used"

		% agree	n
Gender	Female	20	552
	Male	18	540
Age	16-24	38	147
	25-39	25	341
	40-54	12	301
	55+	10	303
Ethnic group	Asian	29	233
	Black	23	44
	Mixed	28	48
	White	13	698
Country of birth	UK	19	852
	Outside UK	20	213
Social class	ABC1	21	644
	C2DE	16	449
Recent victim of crime	No	24	896
	Yes	17	167
Total		19	1093

Note: Percentages calculated with missing values excluded
Weighted data

The potential 'chilling' or 'warming' effects of LFR were further explored in the telephone interviews. Again, most respondents stated use of LFR would not discourage them from going to public events. Some reasoned this was because they were not on the police's 'watch list' and therefore had 'nothing to hide', while others could appreciate the potential safety benefits of LFR, such as a reduction in the threat of terrorist attacks.

It was also reasoned that there are currently other types of surveillance being used across London, such as CCTV and automatic number-plate recognition, and LFR was considered to be merely an extension of this through the use of more sophisticated software.

"It would actually make me feel a lot safer knowing there was AFR."

"I think in this day and age, with CCTV cameras everywhere I have become used to this sort of thing."

Most of the respondents who would not stay away from LFR-monitored events said they considered the technology to be appropriate for all types of public events. Furthermore, a few even felt it could also be used in other public places such as train stations, airports and shopping centres. However, some said they would 'think twice' about going to small gatherings and political demonstrations if they knew it was being monitored by LFR. These participants felt the use of LFR could only be justified at very large, corporate events such as football matches and stadium music concerts.

A small proportion of respondents were opposed to the use of LFR at public events. Others, although not against it, had some concerns. The main issue was that people did not like the idea of their actions being monitored and likened it to being watched by 'Big Brother'. Furthermore, some felt that operating LFR at public events would be a precursor to it being used more widely across London in the future. Some participants were also suspicious of the police using the information to track the activities of political protestors, as well as targeting certain groups (e.g. ethnic minorities). In addition, the accuracy of the technology and potential for mistaken identity was discussed, along with scepticism that images of innocent people will indeed be discarded.

"My main opinion is that I think it is extremely intrusive; it doesn't fit in with the idea of living somewhere that isn't a police state."

"It is effectively the same as asking everyone to give their fingerprints, DNA or to show their driving licence, but in a way that is more covert...I think you would have to weigh up whether you really want to go to that event."

The results from the survey indicated that Asian respondents were more likely to say they would stay away from events monitored by LFR. In the follow-up interviews, the main concerns among Asian respondents mirror the general issues presented above: potential data misuse, data security, accuracy of the technology and LFR potentially being rolled out on a wider scale. However, concern around these specific areas was seemingly higher among these participants. One possible reason for some Asian respondents expressing more reserved views around the use of LFR at public events may be because of their knowledge and/or experience of countries which have prominent 'surveillance states', such as China. Indeed, a few Asian participants explained they did not want to feel 'like I am being watched' and were fearful the use of LFR would eventually be used by the government to 'control and spy on the population'.

"I am Chinese, so from my origin surveillance is quite a big thing. For me, coming to a different country, I want to feel that people don't need to feel fearful of their government."

How far do Londoners trust the MPS to use their personal data responsibly?

Irrespective of any decision to deploy or not deploy LFR, new digital capabilities and technologies will inevitably entail the police gathering, using and analysing ever-enlarging quantities of personal data. The adoption of future technologies such as other biometric identification tools, analytic software for investigation of offences with a 'digital footprint', and predictive policing algorithms will vastly increase the data the police hold. We therefore explored how far Londoners trust the MPS to use their data properly. **Figure 3** displays the percentage of people reporting agreement with a range of statements regarding how data are collected and used.

Notably, only 56% of those we surveyed thought that police would use their personal data in accordance with the law. Between two thirds and four fifths of respondents wanted control over their personal data and felt police use of it should be constrained. Fewer than half agreed with the routine collection of personal data, in relation to crime or non-crime related issues.

People's trust or distrust of police use of personal data was further explored in the interviews. Around half of respondents doubted that the police would use their personal data responsibly and lawfully. Some reasoned they had lost confidence in the service due to negative stories in the media, while others explained that human error does happen and they doubted the systems currently in place would prevent individuals from (intentionally or unintentionally) mishandling or misusing information.

> ***"They go through protocols and if they do something wrong then no doubt it would be picked up."***
>
> ***"It is not something I would trust our police forces with because they have a history of misusing information."***

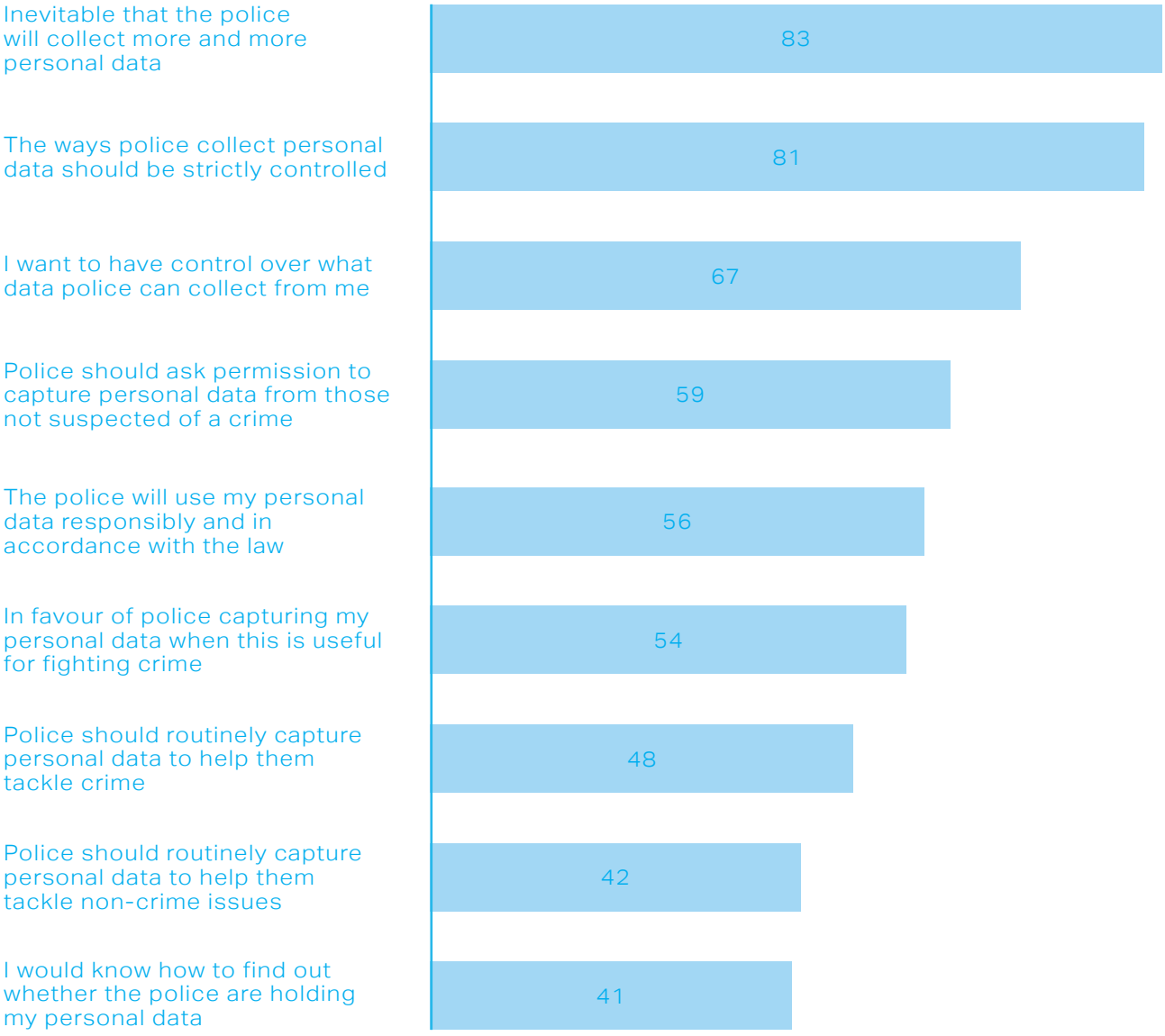
When asked to outline their main concerns with police use of personal data captured by LFR specifically, some expressed reservations and sought reassurances. Several participants highlighted their lack of trust that police would collect information from LFR which only related to offenders. Specifically, there were questions around what exactly was meant by 'people of interest to the police' and there were concerns around data being used for targeting groups of people based on their political affiliation, race, and/or past criminal convictions. A few questioned whether regulations around how LFR data is used could allow the police freedom to monitor a wider group of people and pass on information to third parties.

There were additional concerns around whether LFR would be managed by an external organisation (similarly to speed cameras), rather than the police, which may result in information being used to generate revenue rather than apprehend criminals. It was also felt that more information was needed around how images of innocent people would be discarded (e.g. whether they would be permanently deleted or kept in a separate file and not used). The importance of the public being made fully aware of LFR and being able to give (or withdraw) their consent to having their face scanned was also discussed.

> ***"I trust [the police] to adhere to the rules, but it is more how these rules are applied and utilised."***
>
> ***"I think the issue is when your face is scanned you don't actually know that your personal data has been taken so it is difficult to follow up."***

Finally, using our survey data we were also able to explore whether there was an association between attitudes relating to trust in the police and peoples' current views on the acceptability of LFR. We divided our sample into three groups: high; medium and low trust.[10] Around four in five of those high in trust thought police use of LFR was acceptable, compared with less than three in five of those with 'medium' levels of trust and only two in five of those low in trust.

FIGURE 3: PERCENTAGE AGREEING WITH GENERAL VIEWS ON POLICE CAPTURING PERSONAL DATA



10. The three groups were created by, first, generating a scale from items contained in the survey that related to trust in the police. On this scale, high scores indicated greater trust. The 'low trust' group was defined as those who scored one standard deviation or more below the mean level of trust, while the 'high trust' group was defined as those who scored one standard deviation or more above the mean.

Implications of our survey for LFR and future policing technologies

Those we surveyed were for the most part supportive of police use of LFR when it is targeted at preventing serious crime or apprehending serious criminal offenders. However, support is by no means universal or unconditional. Levels of support for using LFR decrease as the perceived seriousness of the offence diminishes. Additionally, many people expressed significant concerns about privacy, and do not necessarily trust the police to use such a potentially intrusive new technology appropriately. The potential 'chilling effect' of LFR on people's use of public spaces is also of concern, particularly among younger individuals and some ethnic minority groups.

Trust formed an important lens through which participants in the survey viewed LFR. Those who trusted the police were much more supportive, perhaps particularly because they thought the police would use the technology and data properly and appropriately and could make policing more efficient and effective. Yet, both the on-line survey and follow up interviews suggest limits. People are also concerned about controlling their own data, the extent to which police might work with other agencies that have access to the data, and the need for transparency. If LFR were to be adopted care would be needed to ensure that the ways that LFR were used did not serve to undermine trust in police and policing more broadly.

Implications for future technology development

Turning to future development processes, it seems likely to hold true that trust will form the prism through which people view police technology developments. In particular, if they view police as well intentioned – aiming to do the right things for the right reasons – they may be more likely to accept take up of new technology, even if they do not necessarily understand either the tools involved or how police will use them. We can draw by analogy from research on public acceptance of new technologies such as gene editing or nanotech. This regularly finds that people who trust those developing and using new technologies (for example, people who trust scientists) are much more accepting of new technologies than people who lack such trust.

For this reason it would appear prudent to ensure that steps are being taken now to build and maintain the public's trust in police use of new technologies, and in police commitment to 'algorithmic justice' (discussed later). This would mean ensuring robust governance of technology field trials, transparency about decisions regarding adoption of new technologies, and dialogue with the public about how technologies should be used. We argue that there is value in imposing self-limiting constraints, in the interests of building trust and gaining implied consent to adopt new technologies potentially supportive of policing in the public interest.

3. HOW SHOULD TECHNOLOGIES BE TRIALLED IN FUTURE?

Engaging citizens in field trials of policing technology requires an ethical foundation. In our Interim Report we made thirteen recommendations to enhance governance of the Live Facial Recognition trials. The MPS trials have now been completed, but understanding gained from the LFR trials can be used to improve the way in which future technology field trials are designed, operationalised and governed.

As other technologies become available, including new modes of surveillance and tools that draw on machine learning algorithms, these will undoubtedly present further challenges for ethical testing in the field (Oswald et al., 2018, Babuta et al., 2018).

To the extent that policing technology trials are akin to field research, they should observe established ethical precepts designed to protect human subjects from harm in the course of research. The central protective principles are avoidance of harm and coercion. The conventional basis for engaging human participants is therefore through eliciting voluntary participation on the basis of informed consent; or, where this is impossible, by offering a compelling justification for modifying or dispensing with consent. On the other hand, to the extent that field trials of policing technology are a police operation, they will be governed by the usual ethical principles that apply to policing interventions, including accountability, legality, necessity and proportionality. We recognise that ethical precepts governing field research and the ethical precepts governing policing activity may in some respects conflict, particularly over what may constitute legitimate grounds for coercion.

The Panel is supportive of the development of evidence based policing, which presupposes good field research. Field trials are of value to test whether a technology can effectively serve valid policing aims, whether expenditure on it is likely to be a good use of public funds, and whether it supports economical use of limited policing resources. In this section we therefore propose a framework for ethical conduct of field trials of new policing technology. We argue that they must serve the public interest; be sufficiently well designed to be of scientific and operational value; respect equality, dignity and human rights; and be responsive to public concerns generated in the course of the trial.

Issues raised by the LFR trials

Our interim report drew attention to a number of issues that arose during the LFR trials. These have informed our view on issues to be taken into account when conducting technology trials in future.

- ***Conceptualisation and design of the field trials.*** We queried whether aspects of the field trials could have been achieved in simulated conditions, without the need to involve the public. We noted that while MPS was intending to test the operational utility of LFR, it was not clear to what policing purposes the technology could potentially be applied in future. This made it difficult to evaluate the technology's capability in situations in which it might in future be deployed, or to anticipate ethical issues that might be raised by such deployments. We also discussed the difficulty of identifying criteria for success, in that either the presence or the absence of arrests or other criminal justice outcomes might be regarded as successful policing. Additionally, we queried the selection of trial situations, emphasising the need to avoid apparent bias in testing the technology in predominantly minority ethnic events or communities.
- ***How members of the public were engaged in the field trials.*** We raised concerns regarding the extent to which the public were provided with information about the trials, whether they engaged voluntarily, and whether avoiding being scanned would incur any coercive response. MPS subsequently clarified that declining to be scanned would not necessarily be viewed as suspicious. However, we are aware that during one field trial a fixed penalty notice for a public order offence was issued to a pedestrian who avoided the camera by covering his face, and subsequently swore at police officers who sought to engage with him. We discuss the implications of this case below.

- ***Avoidance of harmful consequences of novel technology.*** We drew attention to concerns about the accuracy of the LFR technology and the potential prejudicial impact of inaccurate recognition. We acknowledged concerns that the technology might less accurately identify members of ethnic minority groups.
- ***The legal foundation for deploying novel technologies*** We identified concerns regarding the regulatory confusion surrounding LFR and analogous technologies, which engage in different ways the remit of the Biometrics, Surveillance and Information Commissioners. The MPS subsequently published its analysis of the legality of its LFR deployments and the Surveillance Camera Commissioner has provided guidance augmenting the Surveillance Camera Code of Practice. However, developing technologies have a tendency to outrun legal constraints and the regulatory complexity persists.

Designing field trials of policing technology

It is a defining characteristic of new technologies that their potential benefits and harms are unknown, their uses experimental, and their eventual reach unpredictable. This makes evaluating them in an operational context extremely challenging, and the corresponding ethical issues complex.

The starting point however is that a trial involving human subjects, and using public resources, should produce worthwhile knowledge. There is no ethical validity to trials that are poorly designed, inadequately rigorous, repeat earlier work, or fail to answer the most pressing questions. Policing field trials should be designed in ways that reflect that the police can exert considerable power over citizens, that policing is a public service and that policing technologies may have wide and unpredictable effects.

Trial design and public service

The first task is to conceptualise the potential in the innovation to be tested, the rationale for a proposed trial, and the likely effects on those whom the police serve. The ways in which technologies are presented, programmed, managed, evaluated and implemented affect people in ways which are both deliberate and inadvertent (Winner, 2010) Trust can potentially be enhanced or compromised by the ways in which a technology trial is conceived, planned, and executed.

We suggest that, however knowledgeable the team that is assembled, those working within policing cannot anticipate all of the implications of a novel technology for all those whom it might affect. Moreover, policing is a public service to many different communities, in which there are likely to be diverse views on the effects of novel technologies. An inclusive approach to articulating and planning a trial, involving different voices and external perspectives from the outset, will help generate a robust trial design and hence enhanced ethical validity.

Where it is possible to do so, engaging in an open way with the public from the earliest stages of considering a novel technology reflects regard for others, respect for divergent views, recognition of the nature of service and a commitment to ongoing dialogue and learning.

Designing for scientific and ethical legitimacy

Little has been published on researching novel technologies in a criminal justice context, and what constitutes ethical practice when the police are considering trials or evaluations of technologies of interest. We have therefore drawn from the literature on research into novel technologies, notably the work of Van de Poel (Van de Poel, 2016)

Police field trials of novel technologies potentially have more in common with the concept of a 'social experiment' than they do with conventional biomedical or social research. A true social experiment is a randomized field trial of a social intervention. But some definitions emphasise the 'field trial' element rather than 'randomization', so that at its core a social experiment tests a prospective intervention on a small scale before it is widely adopted (Weiss and Birckmayer, 2006). The scale and nature of the social intervention may make it difficult to gain agreement from every individual in a community affected by a trial. And social experiments can be as much a process of implementation as they are a process of testing.

Established ethical principles present in international conventions governing experimentation with human subjects (notably the Declaration of Helsinki)[11] nevertheless provide a basis for a modified set of principles to be applied to field trials of novel technologies.

Van de Poel has set out a framework of sixteen 'principle-based conditions' (table on this page) for trialling novel technologies in ways akin to social experiments and we found these a useful starting point for considering trials of novel technologies in policing.

VAN DE POEL'S PRINCIPLES	
1	Absence of other reasonable means for gaining knowledge about risks and benefits
2	Monitoring of data and risks while addressing privacy concerns
3	Possibility and willingness to adapt or stop the experiment
4	Containment of risks as far as reasonably possible
5	Consciously scaling up to avoid large-scale harm and to improve learning
6	Flexible set-up of the experiment and avoidance of lock-in of the technology
7	Avoid experiments that undermine resilience
8	Reasonable to expect social benefits from the experiment
9	Clear distribution of responsibilities for setting up, carrying out, monitoring, evaluating, adapting, and stopping of the experiment
10	Experimental subjects are informed
11	The experiment is approved by democratically legitimized bodies
12	Experimental subjects can influence the setting up, carrying out, monitoring, evaluating, adapting, and stopping of the experiment
13	Experimental subjects can withdraw from the experiment
14	Vulnerable experimental subjects are either not subject to the experiment or are additionally protected or particularly profit from the experimental technology (or a combination)
15	A fair distribution of potential hazards and benefits
16	Reversibility of harm or, if impossible, compensation of harm

We have used these principles to develop a proposed framework for field trials of policing technology, set out below. First however we address two critical questions. These are whether citizens can be compelled to participate in policing technology trials; and how their voluntary participation is elicited.

Compulsory participation?

We acknowledged earlier that the ethical precepts governing field research and the ethical precepts governing policing activity may in some respects conflict, particularly over what may constitute legitimate grounds for coercion. We also note that Van de Poel's framework envisages that experimental subjects (which in police field trials means ordinary citizens) should be able withdraw from the experiment.

The voluntariness of participation presents a particularly thorny problem for police field trials, combining as they do an experimental situation with the exercise of police powers. An ethical approach to police technology trials cannot sidestep this problem. We believe the MPS was right to state to the public that declining to be scanned would not necessarily be viewed as suspicious. However, as noted earlier, during one field trial a fixed penalty notice for a public order offence was levied on a pedestrian who avoided the camera and subsequently became involved in a heated exchange with police officers who intervened. We do not wish to focus on the detail of this case, but to use it to set out the principle that we argue should apply.

The correct principle, in our view, is that a police field trial should not create additional legal hazard for members of the public, over and above that to which they would otherwise be exposed. This means that merely avoiding the technology on trial should not prompt an intervention.

We would argue that this principle is the same as that applied in the exercise of police 'stop and account' powers, whereby a refusal to stop cannot of itself constitute grounds for suspicion justifying further action.[12] A refusal to be in a field trial should not of itself be treated as grounds for suspicion. The threshold required to be reached should be the usual grounds for stopping and searching, or carrying out an arrest.

What is required to demonstrate that participation is voluntary?

In much conventional research there is an expectation that participants will give 'informed consent'. These means that potential participants should be given intelligible information about the project, told about risks and benefits, and have an opportunity to agree or refuse to take part.

However, in a policing field trial (as with many social experiments) it may not be feasible to elicit explicit consent from everyone, including affected groups and communities. Moreover, in a trial of novel technologies it is more problematic to articulate risks and benefits with confidence, because of the uncertainty that surrounds the technology's potential. An alternative approach is required in order to meet the same aims of protecting subjects from harm, respecting their rights and acknowledging legitimate preferences.

Arguing from the perspective of engineering ethics, Martin & Schinzinger (Martin and Schinzinger, 1989) proposed two conditions that might substitute for informed consent where trialling novel technologies made informed consent impossible. Where individuals cannot be readily identified, at the very least "information that a rational person would need, stated in understandable form, has been widely disseminated" and agreement or permission, agreement to participate may be obtained by proxy from "a group that collectively represents many subjects of like interests, concerns, and exposure to risk" (p.87)

However, policing technology trials are arguably more sensitive than engineering trials. A more scrupulous information standard has been proposed by Introna (Introna, 2005) who argued that 'disclosure ethics' are essential to social experiments with novel technologies such as facial recognition. The standard requires more than merely sharing information and uncertainties at the outset. It involves continuing moral consideration of the issues at stake at each and every stage of a trial. It requires investigators to identify the values embedded in specific technologies and the value choices made in decisions to trial them; considering at every stage what sort of information needs to be disclosed and to whom; and committing to wide dissemination of questions and findings so that they are available to all who might be interested.

Adopting the perspective of disclosure ethics, the Panel considers that principles of accountability, openness, partnership work, and dialogue should inform the approach to securing valid participation in field trials of policing technology. This is reflected in the ethical framework we propose below.

Whilst advocating for openness and inclusivity, we recognise that for reasons of security there may be situations in which it is not possible to be wholly open about a technology being trialled. In such circumstances, consultation with a group such as Martin and Schinzinger propose, able to represent the interests of potential subjects without jeopardising security interests, would be of value. We would however urge use of this 'security privilege' sparingly, and only where absolutely necessary.

A proposed ethical framework for field trials of new policing technologies

In this section we offer a framework for designing field trials of policing technologies. We suggest it is applicable to all trials of policing tools or policing technology that will involve the members of the public. We have designed it as a guiding structure to support discussion and judgement, and enhance the ethical validity of future trials.

We view the guiding values shown on the left-hand side of the table as critical to maintaining trust in policing in the course of trialling new technologies. They should be considered against the three dimensions of individual impact, group effects, and wider public interests. The questions we have set out are intended to be illustrative, not exhaustive, and not all of the questions will be relevant to every technology or proposed trial.

We recommend that when designing and conducting future trials of new policing tools and technologies, MPS incorporates consideration of this ethical framework into its planning processes.

11. https://www.wma.net/policies-post/wma-declaration-of-helsinki-ethical-principles-for-medical-research-involving-human-subjects/
12. https://www.gov.uk/police-powers-to-stop-and-search-your-rights

Domain	Value or Principle	Considerations for trialling new tools / technologies		
		Individual	Special group interests	Wider public interests
Serving the public	***Openness***	How will we communicate with everyone who may be interested in or affected by a proposed innovation or trial?	Do we have strategies for communicating and/or working with particular groups of stakeholders, including people who are less able, vulnerable, or stigmatised?	What governance structures do we need to have in place to promote protect public interests?
Serving the public	***Inclusivity***	What mechanisms can we use or develop to solicit individual views, participation, or feedback to enhance trial design, governance, or findings?	How can we reach all those we need to? Whose voices are not being heard, and does that matter?	In what ways – if any – is the public interest in the innovation currently addressed in policy, regulatory, political or other representative activity? How will we take this rang e of perspectives into account?
Serving the public	***Engagement***	How will we give consideration to the full range of individual views about innovation or trial, including views that are not supportive? How will we explain our conclusions?	Does our approach to engagement reflect the needs of specific groups and communities?	Does our approach to public engagement in the trial reflect the benefits of dialogue and partnership with others? Is it consistent with good practise for public service organisations?
Serving the public	***Maintaining trust***	How might this innovation or trial affect perceptions of policing and individuals' trust in the police? How might it increase or reduce trust? How should we address this?	How might this innovation or trial affect trust in the police in different communities? Might it increase or reduce trust? How should we address this?	What are the potential implications of this innovation or trial for policing by consent? Who is accountable for ensuring that any trial is legally and ethically sound?

Domain	Value or Principle	Considerations for trialling new tools / technologies		
		Individual	Special group interests	Wider public interests
Robust trial design	***Trial is purposeful and well designed***	Can we assure individuals likely to be affected by it that a trial is necessary, that its purposes are clear, and that it will answer essential questions about how using the technology in policing operations will enhance public protection?	How might the knowledge created in the trial impact differently on different groups or communities?	Does the trial design answer valid and necessary questions about the innovation's use in policing operations? Have we considered public interest concerns regarding the innovation or trial? How will the trial address questions prompted by those concerns? How will new knowledge be shared?
Robust trial design	***Risks and benefits have been weighed***	Could this trial pose risk (including risk of injustice) to participants / employees / anyone else? How will we mitigate these risks? If we cannot mitigate them, how do we justify asking people to participate?	Does this trial pose different risks to particular groups or communities? If so, how will we mitigate them? If we cannot mitigate them how are they justified (e.g. is there any commensurate gain for a community)?	Does our governance framework provide for consideration of risks and benefits, including the possibility f new risks or benefits becoming apparent during this trial?
Robust trial design	***Trial is underpinned by expertise and sound judgement***	How have we ensured individuals involved in design operation of the trial possess requisite expertise (e.g. operational policing, legal, ethical, technical knowhow)? Is it clear where they have discretion to act and may be required to exercise judgement? Have they been given sufficient briefing, training or support to make wise and effective judgements when called upon to do so?	Have we involved interest groups, expert communities and local communities to ensure that widest possible range of knowledge and expertise and feed into the trial?	How do we ensure the operation of the trial reflects our commitments to policing by consent, fairness and justice, particularly where discretion is to be exercised?

Domain	Value or Principle	Considerations for trialling new tools / technologies		
		Individual	Special group interests	Wider public interests
Respect for equality, dignity, human rights	***Trial respects diversity***	How have we taken into account the different needs and legitimate preferences of individuals likely to be affected by a specific innovation or trial?	Have we considered how this innovation or trial might impact on different groups in society? Might it benefit them or harm some more than others?	How have we taken into account the wider social, political and cultural implications of this innovation or trial?
Respect for equality, dignity, human rights	***Trial is free from bias***	Have we considered how the innovation or trial design could give rise to unjustified differences (bias) in the treatment of individuals? What steps have we taken to ensure fairness to all individuals affected by a trial?	Have we considered how the innovation or trial could give rise to unjustified differences (bias) in the treatment of particular groups? Are there groups or communities who could be differentially burdened by the operation of a trial? How will these burdens be mitigated?	Have we considered what biases, conscious or unconscious, might be embedded in the innovation (e.g. biased algorithms)? What have we done to counteract possible bias where evidence of this exists? What will we do if evidence of bias emerges during a trial?
Respect for equality, dignity, human rights	***Participation in trial is not coerced or invasive***	Have we considered the ethical basis on which individuals will participate in a trial? Can they make an informed choice whether to participate? If not, what is our ethical justification for involving them? What protections do we need to put in place to avoid illegitimate coercion, invasion of privacy or violation of other rights?	Have we considered where there are vulnerable groups (e.g. those who have been traumatised or who lack capacity) who require additional protection from unwitting participation? What measures should be put in place for them?	Are we complying with regulatory and legal requirements intended to protect the public from coercion, invasion of privacy and other rights?
Respect for equality, dignity, human rights	***Interference is proportionate***	Have we identified the range of individuals whose rights may be affected by an innovation? Could we explain to them how it will be used, and how this is proportionate to problem(s) it addresses?	How does a given innovation or trial sit alongside other policing, public authority or private sector security activities that affect or influence different groups and communities?	Have we considered proportionality across likely proposed users, and compared this with other judgements we make about proportionality?

Domain	Value or Principle	Considerations for trialling new tools / technologies		
		Individual	Special group interests	Wider public interests
Concerns and outcomes	***Trial is subject to continuing ethical appraisal***	How shall we support the continuous development of ethical capability in all those involved in conducting the trial, and promote continuing ethical reflection during the trial?	How can we ensure the views of stakeholders inform continuing ethical reflection during a trial (e.g. consultation, participation in review meetings)?	How do our governance mechanisms accommodate ongoing ethical appraisal?
Concerns and outcomes	***Trial is responsive to emerging concerns***	What mechanisms can we use to enable individuals (public or police), to raise concerns or questions (including ethical concerns) as a trial proceeds?	What mechanisms can we use for groups to raise concerns or questions as a trial proceeds?	What provision will we make to respond to concerns or questions raised about the innovation or trial as it proceeds? Have we identified points at which decisions to continue, modify or halt the trial can be made? Under what circumstances might we call a halt to this trial?
Concerns and outcomes	***We put things right if they go wrong***	How might individuals be adversely affected by the innovation or trial, and what provision should we make to attend to their needs if this occurs?	What provision have we made to attend to the needs of groups who may be adversely affected by the innovation or the trial?	Have we considered how untoward trial outcomes might adversely affect trust and confidence in the police, and how this might be restored? What will we do if these ethical principles (or others) are breached, through error, poor judgement or for other reasons?

4. ETHICAL CONSIDERATIONS AND PROPOSED CONDITIONS FOR USING LFR

We do not yet know whether the trials have demonstrated LFR will be operationally valuable. Assuming that they do, we have come to the view that there are important ethical issues to be addressed but these do not amount to reasons not to use LFR at all. We argue therefore that MPS should proceed with caution and ensure that robust internal governance arrangements are in place that will provide sound justifications for every LFR deployment.

Proposed conditions

In summary, LFR should only be deployed where the following five conditions can be met.

1. It can be shown that the use of LFR offers more than marginal benefit to the public, sufficient to compensate for the potential distrust it may invoke.

2. It can be shown from trial data (and other available data) that the technology itself will not import unacceptable gender and racial bias into policing operations.

3. Controls on use are sufficiently robust to ensure that each LFR deployment is appropriately assessed and authorised, when it is judged both necessary and proportionate to use it for a specific policing purpose.

4. It can be shown that human operators will be knowledgeable about the potential injustices that may be caused by an inappropriate response to identification alerts, that they know how to avoid these, and are accountable for their actions.

5. MPS and MOPAC develop robust governance and oversight arrangements that balance the technological benefits of LFR with their potential intrusiveness. These should meet the Home Office Biometrics Strategy's requirement for transparency, take into account guidance from the Surveillance Camera and Biometric Commissioners, and compensate for the limited powers of the Surveillance Camera Commissioner to inspect, audit or enforce compliance.

Such provision would include:

   a. operating procedures that govern the compilation of LFR watch lists, including provision for ensuring that data are accurate, current, and limited to the agreed policing purpose for the deployment;

   b. operating procedures that govern authorisation and deployment of LFR ensuring its use is legal, necessary, and proportionate on each occasion;

   c. provisions for transparency regarding LFR deployments, for example through publishing data in respect of LFR deployments on MPS's public facing statistics and data dashboards;

   d. oversight by MOPAC in a manner akin to MOPAC's oversight of other potentially intrusive tactics.

We also make three additional recommendations, listed at the end of this section.

In this section of the report we outline our specific concerns regarding LFR, in order to justify the precautionary approach that we are recommending.

Overview of ethical and legal considerations

Since we issued our Interim Report, the Biometrics and Forensics Ethics Group (BFEG) has published a briefing document on LFR outlining a number of issues they believe should be taken into consideration and the Surveillance Camera Commissioner has published guidance on using LFR.[13] There is notable convergence in our respective assessments of the legal and ethical issues at stake, and in potential approaches to managing the risks LFR raises.

The Panel's concerns fall into three groups.

The **first** set of concerns relates to potential injustice and ineffectiveness resulting from the nature of the technology, including the possibility of algorithmic bias and unfairness arising from the way human operators interact with LFR.

The **second** set of concerns relate to possible incursions on civil liberty resulting from decisions about how the technology will be deployed, including the policing goals LFR is used to support and hence the rationale for including citizens on watch lists, the sources of images that will be used, and accountability for decision making.

We discuss both of these sets of concerns in further detail under appropriate headings below.

A **third** set of ethical concerns relate to the strength of protections afforded by current law. Following our Interim Report, the MPS made public its own analysis of the legality of its use of LFR. We do not challenge this legal analysis, although we note that the organisation Liberty is bringing a legal case challenging use of LFR by South Wales Police. Our ethical concerns in this area are akin to those arising in respect of all forms of police surveillance, which are partially addressed by Article 8(1) of the European Convention on Human Rights. This guarantees the right to respect for private and family life, home and correspondence. Article 8 requires any interference with this right to be in accordance with law, and necessary in a democratic society in furtherance of legitimate aims (such as prevention of disorder or crime and protection of the rights and freedoms of others).

UK law including the Regulation of Investigatory Powers Act, Protection of Freedoms Act and Data Protection Act provide the framework to support Article 8. This framework is discussed in the Surveillance Camera Commissioner's guidance, which also notes the protections the European Convention on Human Rights affords to freedom of assembly, freedom of thought belief and religion, freedom of expression, freedom of association, and protection from discrimination in the exercise of those rights.

Given the legitimate concerns that we discuss next, we would argue that police should only adopt LFR technology if it will afford more than a marginal policing benefit in cases of serious crime, whilst being deployed in a way that fully respects the rights protected in the European Convention on Human Rights. We have therefore proposed Condition 1 below.

13. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/781745/Facial_Recognition_Briefing_BFEG_February_2019.pdf

Potential injustices associated with inaccurate identification

One potential source of injustice is the prospect of an inaccurate identification match being triggered, resulting in unwarranted action against individuals. A second is the prospect of a match not being triggered on occasions that it should. Inaccurate identification may be the result of inherent limitations in the technology, or of decisions made by human operators so we deal with each of these in turn.

Technological inaccuracy

The BFEG points that that LFR is a probability based technology, which calculates the likelihood of a match between the captured image from the environment and the image on the watch list. There have been widely publicised concerns in both the scientific community and civil society that there is potential racial and gender bias within LFR systems, the result of under-representation of BAME and female faces in datasets that have been used to develop the technology (Buolamwini and Gebru, 2018). This affects the calculation of probability, an intrinsic bias that could in turn permeate the policing operations in which the technology is used.

Exactly how any intrinsic bias in the technology would infiltrate policing activity will depend on the type of operation in which the technology was deployed; the threshold of probability for triggering an alert; how police officers are trained to respond to alerts; and whether their response is appropriate. As it is not yet clear how LFR technology would be deployed it is difficult to anticipate exactly how bias will feed forward. A lower threshold of probability could potentially lead to unequal and discriminatory treatment against people in those groups more liable to misidentification, who may be stopped and required to identify themselves. A higher threshold of probability would lead to failure to identify people being sought, resulting in inefficiencies and wasted police effort.

It should be noted that while facial recognition technologies are undoubtedly imperfect, so is human recognition capability. Current practice, which incorporates the biases inherent in human operators, is an important baseline against which comparisons should be made (White et al., 2015); but have not featured in evaluations of LFR. It may be that in the long run, with appropriate development of the technology and well-designed protocols for using facial recognition technology, bias could be minimised and justice better served than it is at present.

One of the purposes of the MPS trials was to establish the accuracy of the technology in operational contexts, and to ascertain an appropriate probability threshold for triggering an alert. Rates of false positives (an alert based on misidentification) have been calculated in different ways by different interested parties in this debate, and there has been little discussion of false negatives (failure to generate a valid alert).

We believe it is in the public interest that the data created in these trials are placed in the public domain so that trial findings in respect of technological accuracy may provide evidence for or against anxieties regarding bias and algorithmic injustice. We have therefore proposed Condition 2 below.

The influence of human operators

All that LFR is capable of doing is predicting the probability of a match between a live captured image and an image on the watch list. LFR has been trialled as an assistive technology. When an alert is triggered a human operator, and ultimately a police officer on the ground, must decide whether to take action.

The most immediate and pressing concern for citizens is therefore the prospect of LFR false alerts, where a police officer relying on LFR misidentification decides a match is credible and pursues police action of some sort. Misidentifications that are acted upon by officers are evidently of significance from a civil liberties perspective.

Alerts that are subsequently assessed by officers not to be a reasonable match do not generate unwarranted police actions, and neither do failures of the system to trigger an alert when it should. However, these failures call the technology into question by undermining its effectiveness and potentially resulting in a different variant of injustice.

Deployment in other industries has established how different types of false alert can raise a host of issues in practice. For instance technology users can become prone to 'automation bias'[14] and trust technology to be right without first verifying the accuracy of findings, or, having checked, believe the technology even against their own judgement. Conversely users can respond to high levels of false alerting by ignoring the technology and missing correct alerts. (Parasuraman and Riley, 1997, Cummings, 2004) Evidence suggests training and individual accountability may provide a partial solution but not compensate entirely for automation bias (Bahner et al., 2008, Skitka et al., 2000). Additionally, the BFEG briefing draws attention to the possibility that where the threshold of probability is set too high, and few matches are generated, operators may seek to adjust the setting to generate more, potentially false, matches.

A second purpose of the LFR trials, and the justification for testing LFR in the field, was to better understand how it would function in policing operations. Observers have been present to study how human operators interacted with the technology, and how well the technology has performed in use.

As the manner in which human operators act on identification alerts is a source of potential injustice, we believe there is a public interest in also placing the observational findings in the public domain. Further, human operators (whether police officers or police staff) should be enabled to understand how their interactions with the technology will be central to its use being fair and just and supportive of policing by consent. We have therefore proposed Conditions 2 & 4 below.

Potential incursions on civil liberty associated with deploying LFR

The LFR trials used dedicated mobile cameras, a bespoke watch-list for each deployment, and significant additional local policing resources. Running each individual trial thus required clear purpose, judgement and additional operational resources. Deploying the technology in this way significantly limits the reach of LFR, a limitation protective of civil liberties. However, the prospect is that as technological capacity develops it may be possible to utilise multiple fixed cameras, to process ever increasing numbers of images on the watch list, and to incorporate work into standard operations. As future uses may not be limited by the circumstances of a trial situation, other constraints may be necessary.

Legality, necessity, proportionality and policing by consent

We note the view of the BFEG and the advice of the Surveillance Camera Commissioner that any deployment of LFR must observe principles of necessity and proportionality, essential if the legal thresholds established by the European Convention on Human Rights are to be met. Neither of these principles could be satisfied by unrestricted use of LFR.

In respect of necessity, we share the view of BFEG and others that in a democratic society individuals have an interest in living their lives without excessive monitoring, and therefore that LFR should only be used only if other, less invasive techniques are not available.

In respect of proportionality, we agree that the benefits to be gained from a deployment of LFR must be proportionate to any loss of liberty and privacy that may be entailed.

Proportionality is a matter of judgement. People can legitimately disagree about the worth of outcomes achieved using LFR, and how they should weigh against possible loss of privacy or other interests. We believe that this is one area in which understanding the opinions of Londoners is of value, as it suggests how they view the gains and losses to them personally.

As we note in our earlier discussion, public opinion cannot be treated as definitive. For instance, the views and interests of those who are in a minority are deserving of protection, and we might also seek to give greater weight to the views of those who are particularly vulnerable either to police action or to lack of police protection.

Notwithstanding the need to treat public opinion with caution, we note that the Londoners who responded to our survey were more supportive of the use of LFR for serious violent offences. There was a clear rank order, with support for using it to identify terrorists and those wanted for serious violence being significantly higher than it is for identifying those wanted for minor crime. The lowest level of support is for using LFR to manage nuisance behaviour. Some four out of five respondents supported using LFR inside a ticketed event at a major arena to identify people wanted by the police for serious violent crimes, while only around two out of five favoured using it to control nuisance behaviour at stations.

We believe that this gives some indication both of how members of the public gauge proportionality, and also of the extent to which there could be said to be a generalised consent to police use of LFR. Broadly, the more serious the crime or threat the more clearly proportionate use of LFR is seen to be; and the less serious the crime or threat the less its use appears consistent with the principle of policing by consent.

We were pleased to see that in its later trials MPS restricted the watch list to those wanted for offences involving some level of violence. It subsequently apprehended suspects for a range of offences including robbery, false imprisonment and kidnapping, and breach of a non-molestation order.[15]

We recognise that setting an appropriate threshold of seriousness of offences presents challenges, and therefore offer a suggestion in Condition 3 below.

Integrity of the databases from which the watch list is compiled

During the LFR trials, most images were drawn from the MPS custody databases, but some were also drawn from other sources available to the MPS. We have three concerns regarding the databases (or other sources) from which images are selected:

the quality of images used to compile the watch list affects the operation of the technology. This issue goes to concerns regarding misidentification above.

the legitimacy of the watch list rests on the legitimacy of databases or other sources from which images are selected. There is long standing controversy about the retention of photographs of unconvicted individuals on the MPS custody database, which has been subject to challenge in the courts and has yet to be finally addressed.[16] Moreover, the ubiquity of images on social media also presents the future possibility that police may seek to capture and use these for the purposes of investigating and apprehending people wanted for serious crime.

any database and watch list must be up to date. We note that during the LFR trials, alerts were triggered when the subject on the watch list was no longer being sought by the police.[17]

The BFEG proposed that the construction of watch lists should be subject to independent oversight and the Surveillance Camera Commissioner has set out several further governance expectations. We have treated watch list management as one element the overall requirement for robust governance of LFR use, which we propose in Condition 5.

The 'chilling effect' of increased police surveillance

We respect the arguments that a range of commentators has made, drawing attention to the possible negative effects on society of increased police surveillance through LFR.[18]

A central objection is that surveillance has the potential to produce a chilling effect on democratic debate and protest, and more generally dissuade people from engaging in legitimate activities in public space.

This chilling effect argument is in part an empirical claim. It predicts that police will use surveillance technologies such as LFR in ways that undermine the exercise of political rights, discourage people from associating with those who are under police scrutiny, or inhibit people from participating in activities that do not meet with social approval. The counter argument is that if LFR or other surveillance technology is deployed only when necessary and proportionate, and abuses prevented, then democratic and social interests will not be violated. The question that then arises is how potential uses will be governed and how abuses will be avoided.

The chilling effect argument is also in part about the value of anonymity and freedom of action in public spaces. For some, the mere fact of surveillance is a diminution of this freedom. The opposing claim is that surveillance technologies help to make public spaces safer for virtually everyone, particularly the more vulnerable in society, and they thus enhance freedom. When we asked participants in our survey what they thought about LFR monitoring of events, and how they would respond, they expressed views on both sides of the argument. A substantial minority (around 1 in 5) thought they might not attend events where LFR was in use. Others told us in interview they might be more inclined to do so, as they would feel safer.

The interests represented on both sides of this argument are important ones. The Panels' view is that if there are significant legitimate policing benefits to be gained from LFR these should nevertheless not be gained at the expense of valued liberties. Given the framework of legal obligations that currently exists, we propose that an appropriate ethical response is to implement robust internal governance procedures that ensure police uses of LFR technology meet, and to some extent surpass, these legal obligations.

14. Cummings, Mary. "Automation bias in intelligent time critical decision support systems." AIAA 1st Intelligent Systems Technical Conference. 2004. Parasuraman, Raja, and Victor Riley. "Humans and automation: Use, misuse, disuse, abuse." Human Factors 39.2 (1997): 230-253.
15. (http://news.met.police.uk/news/arrests-made-during-trial-of-facial-recognition-technology-in-romford-357014?utm_campaign=send_list)
16. www.gov.uk Review of the use and retention of custody images. February 2017. "In 2012, the High Court ruled, in the case of RMC and FJ v Commissioner of Police for the Metropolis and Secretary of State for the Home Department [2012] EWHC 1681 (Admin) 1 ('RMC'), that the retention of images from unconvicted individuals…was unlawful. In response to this judgment, the Government commissioned a review of the current framework for the acquisition, retention and deletion of custody images as well as their operational uses and governance arrangements." A deletion on request policy has been instigated pending the publication of the Home Office Biometrics Strategy.
17. Metropolitan Police Service Press Release Feb 01, 2019 00:19 GMT "Arrests made during trial of facial recognition technology in Romford"
18. See e.g. https://www.libertyhumanrights.org.uk/resist-facial-recognition

Governance and accountability for LFR deployments

We have noted the regulatory complexity that surrounds the use of facial recognition technologies. The Surveillance Camera Commissioner has published guidance augmenting the Surveillance Camera Code of Practice, referring to the relevant laws and the remit of Biometrics and Information Commissioners. However, these bodies have limited powers to inspect, audit, and enforce compliance prior to breach. Given the complex legal landscape, and the relative weakness of national regulatory powers, the choice appears to lie in either passing over the use of LFR or adopting it subject to mechanisms that will help to build public trust, promote transparency and accountability, and sustain robust self-regulation.

If it can be demonstrated from the trials there are clear and legitimate benefits to be gained from using LFR in defined circumstances, the Panel would favour proceeding by way of self-regulation and procedures that promote openness, transparency, and accountability. Below we set out what we believe to be reasonable conditions for use of LFR following completion of the MPS trials. These are not ranked in order of importance. They are set out according to the structure of our discussion above.

Condition 1
The need to demonstrate LFR is of more than marginal benefit

Marginal benefit would not be sufficient to justify LFR's adoption in the face of the unease that it engenders in some, and hence the potential damage to policing by consent. Clearly there is no benefit to be gained from adopting an ineffective technology, and we assume the MPS would not wish to do so. Assuming that a case can be made for deployment, however, we have noted that use of LFR raises legitimate ethical concerns. These should be taken into account when calculating the overall desirability of adopting it.

Additionally, in our survey young people and people from BAME groups were more likely to say that they would stay away from events where LFR was in use. If LFR is genuinely likely to benefit these communities, there is a need to build trust and to make the case for using it.

We propose the technology should not be adopted unless it can be shown from the field trials that it will be able to significantly increase police efficiency and effectiveness in dealing with serious offences, whilst also demonstrating fair, respectful and even-handed use of power. In terms of efficiency, we would note the BFEG argument that it should be considered whether resources required to adopt LFR could be better used elsewhere.

Condition 2
Building trust by making trial data public

We have argued above that it is in the public interest that the data created in respect of technological accuracy during these trials be placed in the public domain, to provide evidence for or against anxieties regarding bias and algorithmic injustice.

Additionally, observational data from the LFR trials regarding the manner in which human operators acted on identification alerts is indicative of how the technology will function in use. These observational findings should also be made public.

Consistent with genuine openness and transparency, we would expect negative as well as positive findings to be included in the trial data that are published.

Condition 3
Necessity and proportionality

Each and every deployment of LFR should be justifiable in terms of necessity and proportionality. We have indicated above that the view of Panel is that this condition is only likely to be met where LFR is used for policing more serious crimes.

We propose below (Condition 5) that LFR use should be governed through a system of robust self-regulation adopting some principles analogous to those found in Regulation of Investigatory Powers Act 2000 (RIPA) and the Protection of Freedoms Act 2012. A threshold for deploying LFR and for including offenders in watch lists should be identified and monitored within this system. One way of determining the threshold might be by reference to minimum terms of imprisonment (e.g. not less than twelve months) analogous to the approach used in RIPA.

Condition 4
Focused training for police civilian operators and officers

Deploying LFR introduces a potentially powerful new form of interference in people's rights, and we have noted above that the way LFR is used by police personnel will have a marked impact on its accuracy, effectiveness, and legitimacy.

The observational findings from the trials, particularly how police personnel respond to alerts and approach the members of the public, should be reflected when developing the standard operating procedures for LFR. The risks associated with operation of the system should be given thorough consideration, and appropriate training for police civilian operators and officers provided in order to mitigate the risks.

Condition 5
Robust voluntary self regulation with independent oversight

LFR can be used both overtly, as it was in the MPS trials, and potentially also in covert operations. These two uses are differently regulated. Overt deployments of LFR would fall under the remit of the Surveillance Camera Commissioner while covert surveillance using LFR would be governed by provisions in the Regulation of Investigatory Powers Act (RIPA) and the Investigatory Powers Commissioner's Office. Covert surveillance operations are subject to more rigorous scrutiny than is overt use of camera surveillance, with each covert surveillance operation individually authorised by an accountable RIPA Authorising Officer.

It is the Panel's view that the potential for intrusion arising from overt deployment of LFR is not negligible. However, we believe that the risks can be mitigated through adopting self regulating procedures equivalent to those that serve to limit intrusion by covert surveillance (derived from RIPA and the Protection of Freedoms Act 2012).

To be clear, we are not arguing that the RIPA Code of Practice, which governs covert operations, be extended to govern overt use of LFR. Rather we propose that processes and procedures governing overt use of LFR should be developed by reference to those elaborated in RIPA, which have been designed to balance security interests with protection of fundamental rights and freedoms. Overt use of LFR in police operations should be governed by an MPS Code of Practice that draws where appropriate on principles set out in the RIPA Code of Practice, the Surveillance Camera Code of Practice, and other relevant protections.[19]

The governance system for LFR deployment should meet the Home Office Biometrics Strategy presumption of transparency,[20] support effective assurance, and promote opportunities for learning and improvement. It should provide for clear lines of accountability, and oversight of LFR deployments by MOPAC.

Key components would include:

a. operating procedures that govern the compilation of LFR watch lists, including provision for ensuring that data are accurate, current, and limited to the agreed policing purpose for the deployment;

b. operating procedures that govern authorisation and deployment of LFR ensuring its use is legal, necessary, and proportionate on each occasion;

c. provisions for transparency regarding LFR deployments, for example through publishing data in respect of LFR deployments on MPS's public facing statistics and data dashboards;

d. oversight by MOPAC in a manner akin to MOPAC's oversight of other potentially intrusive tactics.

We suggest the LFR governance arrangements would benefit from being developed with independent input and from incorporating ongoing public representation.

19. For further comment on regulation of covert uses see the Surveillance Camera Commissioner guidance. We note that the SCC guidance also advocates applying RIPA principles to governance of overt uses.

20. See paragraph 6, p.8

Recommendations

In addition to the conditions listed, we are also making three recommendations. The first of these was proposed in Part Three, and is included here for purposes of clarity.

Recommendation 1
Enhanced ethical governance of policing technology field research trials

We drew attention in Part Three of this report to the challenges of conducting ethical field trials of new policing tools and technologies. Such trials are a hybrid of research trial and policing operation, each of which prioritises different ethical principles.

We have proposed an ethical framework to provide guidance, and recommend that when designing and conducting future trials of new policing tools and technologies, MPS incorporates consideration of that ethical framework into its planning processes.

Recommendation 2
Review public views on LFR after implementation

We have argued that while public opinion does not determine what is ethically acceptable or morally right in any straightforward way, the process of eliciting and seeking to understand Londoner's views on how their city ought to be policed is an important ethical task. It provides insight into the relationship of trust between the MPS and Londoners, identifies how approaches to policing may have different impacts on individuals and communities, and helps to indicate how far Londoners believe the exercise of police power is proportionate to the goals the police are seeking to achieve.

The National Decision Model for policing, which we have found a useful framework to support our own deliberations, calls for actions to be followed by review of their impact. We recommend that in the event MPS proceeds to adopt LFR, approximately 12 months after the first LFR deployment MOPAC should gauge its effects through incorporating elements of the public opinion survey carried out for this report into MOPAC's next quarterly Public Attitudes Survey.

Recommendation 3
Call attention to the need to simplify and strengthen regulation of new identification technologies

It is clearly in the interests of maintaining trust in policing to ensure that LFR (and future analogous technologies) are regulated in ways that are consistent, rigorous, and transparent. In his March 2019 guidance the Surveillance Camera Commissioner noted the limits of his powers, and the different and discrete responsibilities of the Biometrics and Information Commissioners. We believe this situation creates confusion for the public and exposes both the public and the police to varied risks associated with weak governance of fast developing technologies.

As MPS was one of the first police services to trial LFR, and is likely to be at the forefront of testing future technologies, we would argue that MPS and MOPAC have a potentially influential part to play in calling for simplified yet robust regulation. We also consider the College of Policing may have an important role in developing Approved Professional Practice in this area.

Anticipating future technological developments, MOPAC and MPS should continue to draw Home Office attention to the need to simplify and strengthen the regulation of new identification technologies.

5. AFTERWORD - REFLECTING ON NEW POLICING TECHNOLOGIES

It is difficult to predict how new technologies may develop and come to be used. In this report we have focused on LFR, but also asked what can be learned from trialling LFR when other new technologies become available in future.

In this section, we invite you to join us in a thought experiment about the future of police surveillance technologies.

People use thought experiments to gain ethical clarity. Describing an extreme or impossible scenario can help to generate additional insight and stimulate discussion. Here we use a thought experiment to explore what we have heard Londoners tell us they value, and what interests they might seek to protect, if new policing technologies are to be introduced. We're going to imagine a future in which there are many more surveillance technologies available, they are much more advanced than they are today, and London is willing to pay for them.

This thought experiment is not about what we expect to happen. We want to emphasise this in the strongest way. No one has yet developed or proposed using technologies like those we're about to describe. There are laws in place (like the Regulation of Investigatory Powers Act, and the Data Protection Act) that mean it can't happen now. But exaggerating the power and scope of technology helps us to think about what might be at stake with the technologies we do have, to reflect on what aspects of this imaginary future we might want, and which parts would give us reason to reconsider our direction.

It is important to think now about what we want for the future, because information-gathering technologies and systems for automated analysis of surveillance data are improving rapidly. Even if facial recognition technology turns out not to be operationally effective, other technologies – such as voice recognition and micro drones – might be. Once a technology is integrated into police operations, it will likely be used for years to come. If we 'switch on' some new technology for today's London, it will still be in use in the future when things may be very different.

Policing with PanOps: a thought experiment

Imagine a future where surveillance technology has been perfected. In our science-fiction future, surveillance technologies have become so good that they can potentially identify everyone, everywhere, all the time. In prospect is a super-advanced surveillance system, 'PanOps', that can keep track of every person, at every moment, in every public place in London. PanOps is so powerful that it could archive complete visual and audio records of everyone at all times, from the day the PanOps system was switched on for decades into the future.

There are over 10 million people in London on an average day, and we're imagining a future where police super-technology automatically keeps track of each and every one of them.

'Are we imagining that the computers know who all the visitors are too?' Yes. 'Are we imagining that the computers know who's demonstrating outside the House of Commons?' Yes. 'Does the computer hear it when someone yells at their kids on the street?' Yes. We're imagining a London where police technology automatically tracks and records every person, in every location in London—absolutely everywhere, except in private residences. (And even for private residences, PanOps automatically tracks who goes in and who goes out.)

In this imaginary future, a police officer can find out almost anything about people and places in London.

- When a police officer says, 'Show me where Joe Bloggs is right now,' the computer shows Joe Bloggs's location on a map.

- When an officer says, 'Show me everyone that Jane Bloggs has spent time with this week,' the computer instantly displays that list.

- 'Show me everywhere in London where people who have been arrested for weapons are in the same place...'

- 'Show me the twelve people in this Borough who have mentioned illegal drugs the most times this year...'

- 'Show me everyone at that anti-arms demo who's ever been arrested...'

- 'Show me every person who holds public office who entered that sex club...'

Again, we're nowhere near this imagined state of affairs. The point of our thought experiment is to examine our responses to it, and then use these to help us think about the technologies that are likely to be on offer. If it were possible, would we want PanOps? If not, why not? Could we get the benefits of PanOps without its disadvantages? How might thinking about this affect the choices we make about more realistic prospects for extending police surveillance?

What the technology developers think

The developers believe that PanOps will enable the police to do almost everything better - faster, cheaper, and with fewer mistakes. In their view, all the tasks of policing in public spaces would be infinitely easier and more efficient with better surveillance technology.

Consider just one aspect of police work they argue: finding missing persons. In the decade up to 2018 London saw a 72% increase in reported cases. And in 2018 the cost of investigating cases was estimated to be up to £130m each financial year (some thought it was even higher).[21] Most of the people reported missing are vulnerable in some way, like young people in care who have run away, or older people who have become disoriented. In the PanOps system, where surveillance technology is perfect, there are no missing persons. The police can instantly find anyone who is reported missing. So all of those police hours are freed up for other police work.

And better surveillance could mean less injustice. Fewer people questioned about their whereabouts. Less need to stop and search people who have done nothing wrong. Fewer misidentifications. Fewer wrongful convictions, and fewer wrongful acquittals. And think how, with PanOps operating everywhere, all the time, it could even be an effective constraint on misuse of police power or accusations of misuse of power.

The developers know that switching on PanOps won't eradicate crime overnight. Surveillance is just one part of the picture. Surveillance data can only support the operations that the police decide to undertake. The police must still decide what crimes to pursue and what goals are a priority. PanOps can't decide that. And the police will still have to plan effective interventions. PanOps will tell them where people are, and where they have been, but the police will have to decide what to do with that knowledge. So how the police decide to use PanOps will be as important as the technology itself.

But the developers imagine a future when PanOps has been on for years. They believe violent crime would be drastically reduced. In fact, most of the crime that used to occur in public places (unfortunately it won't impact cyber crime) would be reduced. On the rare occasions when it happened, the offender would almost always be caught quickly. The PanOps developers expect people will hardly ever assault each other in public, or steal bikes, or break into houses, because they would know it's almost impossible to get away with it. For the same reasons, public demonstrations would never get out of control. And domestic crimes would be cut too, because although PanOps can't see into private residences it does always know who was in them.

Crime, especially violent crime, can have terrible consequences for victims argue the developers. Would we not want to use PanOps to prevent it? Would we not be prepared to countenance a few disadvantages to have that kind of protection?'

21. https://www.bbc.co.uk/news/uk-england-london-45810539

New Police Surveillance Technologies: Risks and Strategies

To outline the ethical risks of the new police surveillance technologies, we're going to represent the people who have talked to us about their concerns as six characters. Each of these six 'Londoners' is worried about a different kind of danger in the new technologies:

Londoner 1: Public abuse of power
Londoner 2: Private abuse of power.
Londoner 3: Discrimination.
Londoner 4: The chilling effect.
Londoner 5: Use with predictive technologies
Londoner 6: Youthful mistakes

Londoner 1: Public Abuse of Power

Londoner 1 is worried that police surveillance technologies are powerful tools for collecting information on citizens. Their concern is that they could potentially be used by the police or by governments of the future to violate human rights or civil rights, curtail basic liberties, or even undermine the rule of law.

Londoner 1 recognises some people might think this is a bit overdramatic. 'Shops and banks and airports are already introducing better surveillance technologies, so what's the big deal? If Tesco is going to be using facial recognition, who cares if the police have it too?' But Londoner 1 argues new technologies raise ethical issues that are especially serious when they are used by the police instead of by private businesses.

This is for two reasons. First, police surveillance is more pervasive than private surveillance. It covers public areas that people need to use to exercise their political rights, like marching in protests. And spaces through which people must pass when just going about their lives, going to work and meetings and parties and clubs.

So police surveillance is much harder for the public to avoid than private surveillance. Second and even more important, Londoner 1 says, police surveillance is connected to the punishments of the criminal justice system. A shop that uses surveillance technology to catch someone might kick that person out, or even ban them permanently. But what the police can do to a person is much more serious—like detaining them and seizing their property. And the criminal justice system can end up putting a person in prison for years.

Londoner 1 is especially concerned about the potential of these new technologies to undermine citizens' political rights of free speech and protest. Quickly and accurately identifying people who have participated in an anti-government march, for example, would make it much easier to single out protestors for negative consequences. For democracy to thrive, citizens have to feel able to protest government action they believe to be wrong, and do so without fear of reprisal. Currently, protesters enjoy a sense of safety in numbers. This would be lost in an era of total surveillance.

Londoner 1 argues that we need to think carefully about how public abuse of power happens. While many people believe the British state to be generally benign, says Londoner 1, political history teaches us that we cannot be complacent and assume this will always be so. A future government may turn to the police, and their powers of surveillance, to enforce laws that people believe to be immoral or otherwise objectionable. But, Londoner 1 continues, abuse of power need not come from evil intentions in the police or government. Pursuing legitimate aims like public order or prevention of terrorism can tempt public officials to cross the line that marks justifiable uses of power, while genuinely believing that they are doing the best thing for the community. Ever increasing technological capacity opens up ever increasing possibilities for abuse of power.

Londoner 1 has been reflecting on how to check public abuse of power. Democratic politics itself is one safeguard against it. Competition between political parties, monitored by a free press and a citizenry jealous of its political liberties, can constrain the police or the government of the day from weakening basic rights and liberties. Londoner 1 also believes that legislation may have a part to play here. For example, Londoner 1 suggests, perhaps misuse of surveillance technology by a public official ought to be a criminal offence? Laws designed to avert and deal with abuses of power associated with greater surveillance would demonstrate and serve a genuine commitment to protection of civil rights. And while future governments might wish to rescind such laws, they would at least have to muster the political support to do so.

Londoner 2: Private Abuse of Power

Londoner 2 is worried about the private abuse of power by police officers. Police officers misusing their power for private gain is always a danger, believes Londoner 2, but increasing the scope and range of technologies at their disposal might just make it easier.

For example, Londoner 2 says, a police officer in a custody battle with her spouse might use a new surveillance technology to gather embarrassing information about him. Or a corrupt police official might use the technology to blackmail a reporter who has discovered evidence of her corruption. And gathering information is just one side of the coin. It could be equally tempting to destroy surveillance data in pursuit of private gain.

Londoner 2 notes that police services already have systems in place to detect and punish police misconduct. And like other organisations, which handle sensitive data, police services keep track of how their information is accessed. For example, systems can and should automatically log whenever a recording from a body-worn video camera is replayed in a police station. Londoner 2 believes these practices contribute to reducing the dangers of private abuses of power, as staff and officers know that their use of information systems is being recorded.

But, Londoner 2 argues, maybe we're missing a trick here. One of the best ways of reducing the risk of abuse could be to use surveillance technology as part of the solution to the problem of private abuse of power. Londoner 2 notices that surveillance technologies bring with them the potential to watch the watchers. An important potential use for facial recognition or other surveillance technologies could be to monitor police activity inside police stations, inside police vehicles, on police officers' laptops or tablets, or indeed anywhere that police operatives accesses police data. If surveillance systems are to be used on the public, Londoner 2 says, they should also be used within the police service to produce accurate, verifiable, and enduring records of who has used these systems and how.

For Londoner 2, using new technologies to 'watch the watchers' could be effective in countering police misconduct for the same reasons that using them to keep watch on the public could reduce criminality. The presence of systems for detecting and evidencing abuse could deter those who might otherwise act with a wrongful intent. Londoner 2 offers further arguments. Being subject to the same surveillance systems as are used on the public would remind the police of the importance of using their power responsibly. Finally, public awareness that the police are subject to the same powerful surveillance systems as they are could help to build public confidence. Public confidence might be increased even further if the public knew that external bodies charged with holding police accountable for their actions used of the power of new technologies to do so.

Londoner 3: Discrimination and bias

Londoner 3 is concerned that expanding the scale and reach of police surveillance technologies would further entrench discrimination against communities that have historically been unfairly treated.

Londoner 3 notes that some are of the view that policing has long been discriminatory, and has acted on stereotypical views about predisposition to crime in disadvantaged and minority ethnic communities. Their concern is that police surveillance technologies such as PanOps would have the potential to be a 'force multiplier' for whatever discriminatory policing practices already exist. Londoner 3 is especially concerned that existing bias against disadvantaged communities will have been embedded in today's police databases, and may be transmitted to policing practices whenever technologies that draw on these databases are deployed.

'I can see what the developers want to achieve' says Londoner 3, 'but while the technology might be everywhere all the time the police will never be able to be everywhere all the time. They will focus on the areas where they think they are most likely to find illegal activity'. To see the potential for unfairness, Londoner 3 asks you to reflect on how drug laws are enforced. Rich people use illegal drugs as much as poor people do, Londoner 3 argues, but you are apt to find crime where you look for it. Because police activity has tended to target public drug dealing and visible drug use in poorer communities these crimes are detected there more often - even though rich people are probably breaking drug laws just as much. Focusing policing activity in disadvantaged communities has meant more crime is discovered there, and this reinforces the view that people living in those communities are more likely to engage in criminal behaviour. In Londoner 3's view this would provide an unfair justification for even more scrutiny when PanOps was switched on.

Londoner 3 makes a further point, which is about how surveillance such as PanOps concentrates on visible crimes. Londoner 3 thinks that white-collar crimes, including cyber crime, are just as threatening to the social fabric as those that happen in public spaces under the scrutiny of PanOps. Will investing in surveillance technology for public spaces mean that more police resource is concentrated on policing people in disadvantaged communities, and less on policing high tech white collar crime? Which is more important to society, Londoner 3 asks?

More, Londoner 3 says, we have to remember that every individual Londoner has rights. Even if a majority of Londoners want a new surveillance technology to be switched on, that doesn't automatically make that the right thing to do. Will communities that have historically been discriminated against benefit from PanOps? Or will it just increase the burdens on them? If policing really is by consent, the service will need to make extra efforts to gain the support of communities that fear new surveillance technologies will be used against them, rather than in their interests.

Is there anything that could be done to mitigate the risks of discrimination or bias? Londoner 3 thinks that a partial solution might be more transparency. Whilst PanOps would be on all the time, the police would still be making decisions about where, when, and how to use the data it provides them. Surveys show that members of minority groups, who are most likely to be harmed by any unjust discrimination, tend to be the Londoners who are least trusting of the police. To build greater trust, Londoner 3 would favour a strong default rule that police should share information with public bodies – for example local councils, academics, and civil society organisations – about how PanOps and other technologies were being used to support their policing operations. This would provide grounds for ongoing debate about whether the benefits and burdens of greater surveillance are evenly distributed across London's communities.

Londoner 4: The Chilling Effect

Even with a police and government that were absolutely scrupulous in using PanOps fairly, the introduction of such technologies could have negative effects by limiting what people are willing to do in public. What Londoner 4 is worried about is this 'chilling effect.'

Londoner 4 argues we have to seriously consider that living in a city policed with PanOps may make people think twice about engaging in perfectly legal activities. And if they stop doing what they have a right to do, this may reduce their personal autonomy and harm their relationships with each other. For example, people who believe that they are being watched by police surveillance may be less likely to:

a. exercise their political rights. Suspicions about how the new technologies are being used may, for example, may make people hesitate to participate in legitimate protests against the government—or may even make them think twice about voting.

b. exercise their associational rights. Surveillance may deter people from getting together with those they believe are subjects of special state scrutiny, or with those they believe are associated with such people. Should I worry about visiting a family member if the police have reason to believe they are involved in crime?

c. engage in activities that are perfectly legal, but associated with embarrassment, stigma or shame. Surveillance may deter people from activities they feel perfectly entitled to pursue but none of the business of the state. Group sexual activities such as swinging, for example, are not criminal offences; but participants may feel it is no-one's business but their own to know they take part in them.

To be fair, Londoner 4 says, there would be benefits from 'chilling' criminal and anti-social behaviour. Switching on powerful surveillance technology could have 'warming effects'. Parents, for instance, may feel safer in allowing their children to use public parks and public transport, or attend any sort of public gatherings, if they believe that extra surveillance is in place. Indeed, reducing fear of crime or disorder might make public spaces more welcoming to many.

Londoner 4 concludes that while the police rightly want to focus on how PanOps could help them find specific people engaged in crime, surveillance technologies affect everyone. These technologies always increase the police's power over every citizen, so their use should always come with extra efforts to increase citizens' trust of the police.

What Londoner 4 really wants to emphasize is that the chilling effect is very hard to counteract, because its origin is a distrust of state powers in the form of criminal justice agencies and the government. When people distrust the state, the familiar accountability measures taken by state agencies can't work well. Whatever laws Parliament may pass, whatever oversight agencies might be set up, however transparent the government or the police are, people may not believe they are being told the truth about how much they're being watched or what's being done with that information. When people don't trust the police, they won't trust the police to police the police. And when people don't trust the government, they won't trust the government to police the police either.

Londoner 5: Use with Predictive Technologies

Londoner 5 is aware the developers think total surveillance could drastically reduce crime by making detection and apprehension more likely. But Londoner 5 wonders whether maybe the most powerful way the police will want to use PanOps will be in conjunction with predictive policing techniques. Londoner 5 thinks the police won't want to wait for crime to occur, especially serious violent crime. They would want to use the data they gathered from surveillance activities alongside sophisticated 'predictive policing' algorithms to predict and prevent likely criminal activity.

Some predictive policing algorithms promise to enable the police to predict where crime is more likely to occur. With information about these 'hot spots,' police could deploy resources more effectively to deter crimes. Other predictive policing algorithms could enable the police to predict which members of the public are more likely to be perpetrators or victims of crime. They could use this information to intervene in crime cycles, diverting people away from becoming perpetrators of crime or warning others they are at high risk of becoming victims (for example, of domestic violence).

Londoner 5 is concerned with the possibility that using a suite of new policing technologies in ways that reinforce each other might intensify the risks that earlier Londoners identified.

Londoner 5 shares some of Londoner 3's worries about discrimination, and is anxious that predictive policing could further entrench it. Londoner 5 says that predictive algorithms will be based on data that comes from past policing activity and is therefore likely to have bias built in. Because of this, using them could reinforce a pattern of unfair targeting of disadvantaged communities by the police. But now, 'scientific and objective' computer programmes would justify this biased targeting.

Londoner 5 is also interested in what Londoner 4 had to say about the opacity of state power and the chilling effect. 'I don't think predictive policing alone will have a chilling effect' says Londoner 5, 'but policing algorithms are another example of how new technologies can give the state a form of power that it is difficult for the public to understand, evaluate and challenge.' The prospect of the police using opaque and impervious algorithms to identify and risk-assess 'trouble makers' or victim is, Londoner 5 thinks, rife with potential injustice.

Londoner 5 argues that any technological system which exposes citizens to the exercise of state power against them must be made open to scrutiny by legal and technology experts, and explicable to the public. And Londoner 5 likes Londoner 2's suggestion of using policing technologies on the police themselves. If the police use predictive algorithms to help decide which members of the public are worthy of their attention, they could also be using algorithms to help identify police officers and staff who may be vulnerable to becoming involved in misconduct.

Londoner 6: Youthful mistakes

Londoner 6 is the last to speak up. They found a lot to agree with when Londoner 3 talked about policing of disadvantaged communities, and were concerned when Londoner 5 described how predictive policing could be used alongside surveillance. As a young person, Londoner 6 is all too aware of bad decisions they've made in the past, and the frequent trouble they had with the authorities while they were in their teens and early twenties. They think they have been lucky. With support, they turned things around, gained qualifications and found a job they like. But they still live at home, have some of the same friends, and have siblings who face the same temptations.

Londoner 6 is worried that with a system like PanOps there will be less opportunity in future for Londoners to outrun their mistakes. Londoner 6 fears that once you're in the system as a 'person of interest', or you'll be there forever. And so will the connections to your friends and family and the places you visit. How long will it take, Londoner 6 wonders, for authorities to believe that a 'reformed character' is unlikely to commit or be involved in crime – even if they have been in the past?

Londoner 6 says this is not about being free of the taint of spent convictions, but free of the taint of suspicions. So Londoner 6's challenge is this: they want assurances that PanOps - and any systems associated with it - will periodically be wiped clean of information about people who are no longer involved in activity that could fairly give rise to suspicion. And they also want to know what information is held on them, and be able to insist their own information be removed.

Conclusion

PanOps is of course a fantasy, so how can it help us to understand some of the choices we might make about more realistic technologies? We can use the thought experiment to think about whether we would want the fantasy, why things might not turn out like they do in fantasy, why they just might, and how we would want to deal with what we come to agree are realistic fears.

There are potential benefits to new surveillance technologies, although we think we have exaggerated them here to make the point that using them to support good policing could make a tremendous difference in people's lives. But thinking about the possible benefits points to how powerful surveillance technologies have serious potential risks too. Our Londoners have offered some thoughts about how these risks could be reduced, but there are no simple answers.

The commitment to policing London by consent means that questions about the impact of police surveillance technologies, and the ways they are used alongside other approaches to gathering and analysing crime data, are important to every Londoner. These are not just technical questions, but questions about our values, how we see policing fulfilling its obligations to all of London's different groups and communities, and about what we most cherish in our social arrangements.

BIBLIOGRAPHY

BABUTA, A., OSWALD, M. & RINIK, C. 2018. Machine Learning Algorithms and Police Decision-Making: Legal, Ethical and Regulatory Challenges. Whitehall Reports. Royal United Services Institute.

BAHNER, J. E., HÜPER, A.-D. & MANZEY, D. 2008. Misuse of automated decision aids: Complacency, automation bias and the impact of training experience. International Journal of Human-Computer Studies, 66, 688-699.

BUOLAMWINI, J. & GEBRU, T. 2018. Gender shades: Intersectional accuracy disparities in commercial gender classification. Proceedings of Machine Learning Research, 81, 1-15.

COLLINGRIDGE, D. 1982. The social control of technology.

CUMMINGS, M. Automation bias in intelligent time critical decision support systems. AIAA 1st Intelligent Systems Technical Conference, 2004. 6313.

INTRONA, L. D. 2005. Disclosive ethics and information technology: Disclosing facial recognition systems. Ethics and Information Technology, 7, 75-86.

MARTIN, M. W. & SCHINZINGER, R. 1989. Ethics in engineering, McGraw-Hill.

OSWALD, M., GRACE, J., URWIN, S. & BARNES, G. C. 2018. Algorithmic risk assessment policing models: lessons from the Durham HART model and 'Experimental'proportionality. Information & Communications Technology Law, 27, 223-250.

PARASURAMAN, R. & RILEY, V. 1997. Humans and automation: Use, misuse, disuse, abuse. Human factors, 39, 230-253.

SKITKA, L. J., MOSIER, K. & BURDICK, M. D. 2000. Accountability and automation bias. International Journal of Human-Computer Studies, 52, 701-717.

VAN DE POEL, I. 2016. An ethical framework for evaluating experimental technology. Science and engineering ethics, 22, 667-686.

WEISS, C. H. & BIRCKMAYER, J. 2006. Social experimentation for public policy. The Oxford handbook of public policy.

WHITE, D., PHILLIPS, P. J., HAHN, C. A., HILL, M. & O'TOOLE, A. J. 2015. Perceptual expertise in forensic facial image comparison. Proceedings of the Royal Society B: Biological Sciences, 282, 20151292.

WINNER, L. 2010. The whale and the reactor: A search for limits in an age of high technology, University of Chicago Press.

PANEL MEMBERSHIP

DR SUZANNE SHALE - CHAIR

Suzanne Shale works as an independent ethics consultant. She develops ethical policy and guidance, undertakes commissioned research, provides education and training, and works with organisations to help build and sustain ethical cultures. She has an international reputation for her work helping health care organisations to respond well when patients have suffered harm in their care.

Suzanne is a Visiting Professor at the Department of Security and Crime Science, University College London. Suzanne chairs the UK's leading patient safety charity, Action against Medical Accidents, sits on the Department of Health's Independent Reconfiguration Panel, and is a Non-Executive Director in the NHS. Her book Moral Leadership in Medicine: Building Ethical Healthcare Organizations was published by Cambridge University Press in 2012. She was formerly a Fellow of New College Oxford, University Lecturer in Law, and Director of the Oxford Learning Institute.

Suzanne has spent more than half her life living in London. Moving frequently around south London during her twenties, she helped set up a low-cost housing co-operative. In 1996 she moved north of the river to live in Islington, where she supports charities concerned with mental well being.

PROFESSOR DEBORAH BOWMAN

Deborah Bowman is Professor of Bioethics and Clinical Ethics and Deputy Principal (Institutional Affairs) at St. George's, University of London.

Her background and qualifications are in law and philosophy. Professor Bowman's academic interests concern the application of ethics to professional and practice environments, emotion in ethical decision-making, moral distress, public involvement in ethical debate, theatre and medicine, and therapeutic relationships between professionals and those they serve. She is also a mediator and provides clinical ethics support to the NHS. Professor Bowman has published extensively and she has participated in many international projects in the field of applied ethics and the moral dimensions of public policy and professional regulation.

Deborah Bowman has worked with many national and public organisations. She is currently the Chair of the General Medical Council's working group reviewing national consent guidance for doctors. She also serves as an external member of the General Optical Council's Standards Committee and as a Non-Executive Director of St George's and South West London Mental Health NHS Trust. She is currently a Governor at Morden Primary School. Deborah has a commitment to public engagement and has worked with festivals, theatres, arts organisations, charities and broadcasters, including as Chair of Deafinitely Theatre. She is a broadcaster and regular commentator in the media, particularly for BBC radio. Recent projects include developing and presenting a third series of Test Case and the documentary Patient Undone, both for Radio 4

In 2016, she was awarded an MBE for Services to Medical Ethics. Deborah has lived and worked in South West London since 1992.

DR PRIYA SINGH

Priya Singh's medical career began in general practice, following which she specialised in legal medicine. She has broad strategic and operational executive experience in healthcare and ethics, international member services, professional indemnity and risk. During her career she has advised healthcare professionals on the legal, ethical and regulatory standards underpinning practice in the UK and internationally, including in Ireland, South Africa, Hong Kong, Malaysia, Singapore, New Zealand, Israel, Bermuda, Jamaica, Barbados and Trinidad.

She is a trained mediator and trainer in communication skills, managing change, decision making under pressure and in resolving team conflict. She has particular expertise in quality assurance and governance in the delivery of safe, empathetic and effective patient care. Priya is Executive Director of the Society for Assistance of Medical Families, a mutual provident fund with charity status, a Non-Executive Director of Guy's and St Thomas' NHS Foundation Trust, South Central Ambulance NHS Foundation Trust and an Associate with Working With Cancer, a social enterprise helping those with cancer remain in or return to work. She has lived and worked in Westminster since 1996.

PROFESSOR LEIF WENAR

Leif Wenar is Professor at the School of Law, King's College London, where he holds the Chair of Philosophy and Law. His degrees in Philosophy are from Stanford and Harvard, and he has been a visiting professor at Stanford and Princeton and the Carnegie Council Program on Justice in the World Economy. He is an editor of The Ethics of Philanthropy, and the author of Blood Oil: Tyrants, Violence, and the Rules that Run the World. Since first moving to London in 1998 he has lived in Chelsea and Brixton, and since 2004 in Camden near King's Cross.

1 2 3 4

1. Dr Suzanne Shale
2. Professor Deborah Bowman
3. Dr Priya Singh
4. Professor Leif Wenar.

LONDON POLICING ETHICS PANEL

FINAL REPORT ON LIVE FACIAL RECOGNITION

MAY 2019