MINDEROO
CENTRE FOR
TECHNOLOGY
& DEMOCRACY

A SOCIOTECHNICAL AUDIT: ASSESSING POLICE USE OF FACIAL RECOGNITION

Evani Radiya-Dixit
October 2022

October 2022

This report is authored by Evani Radiya-Dixit, Visiting Fellow, Minderoo Centre for Technology and Democracy, University of Cambridge.

Minderoo Centre for Technology and Democracy

The Minderoo Centre for Technology and Democracy is an independent team of academic researchers at the University of Cambridge, who are radically rethinking the power relationships between digital technologies, society and our planet.

www.mctd.ac.uk

Suggested citation: Radiya-Dixit, Evani, *A Sociotechnical Audit: Assessing Police Use of Facial Recognition* (Cambridge: Minderoo Centre for Technology and Democracy, 2022).

https://doi.org/10.17863/CAM.89953

CONTENTS

FOREWORD

How ethical and lawful is police use of facial recognition?

Many cases demonstrate the need for greater accountability and legislation for the use of such technologies.

The ethics and legality of facial recognition technology should always be at the forefront of any conversation around its use. This problem is especially acute when police and law enforcement adopt and deploy facial recognition tools.

Over the last few years, police forces around the world, including in England and Wales, have deployed facial recognition technologies. Our goal in this report was to assess whether these deployments used known practices for the safe and ethical use of these technologies.

Our report builds on the existing body of research on the use of data intensive technologies in public. We examine the complexities and challenges that exist when police forces use facial recognition technologies.

Building a unique audit system, our report examines the issues of privacy, equality, accountability, and oversight that should accompany any such deployment.

This report results from a year-long research project by our Visiting Fellow, Evani Radiya-Dixit, whose work with us was funded by a Rotary Foundation Global Grant Scholarship. Thanks to Evani's tremendous work on this report, we have a set of tools that can help advance public conversations about the values that we as a society should seek to protect.

At the Minderoo Centre for Technology and Democracy, at the University of Cambridge, we study how digital technology is transforming society, to ensure democratic accountability over the increasing power of tech across the globe. Our research is anchored in creating ways to build capacity in how we as a society can hold tech power systems to account.

We hope that this audit tool and our report will be useful to a wide range of different stakeholders in scrutinising police use of facial recognition technology, and evaluating the use of biometric technologies globally.

Prof. Gina Neff

Executive Director,
Minderoo Centre for Technology and Democracy

EXECUTIVE SUMMARY

Police use of facial recognition technology can pose serious threats to fundamental rights of privacy, equality, and freedom of expression and assembly, especially for marginalised communities.

We propose this sociotechnical audit as a tool to help outside stakeholders evaluate the ethics and legality of police use of facial recognition.

The adoption of facial recognition by police has been the subject of significant debate. Police forces often advocate for the use of this technology to help prevent crime and threats to public security. However, there have been calls for greater accountability and legislation on police use of the technology. Given that police forces continue to deploy facial recognition, we need to assess how police are using the technology today.

Developed for England and Wales, this audit extends to all types of facial recognition for identification, including live, retrospective, and mobile phone facial recognition. We developed this audit using a review of existing literature and feedback from academia, government, civil society, and police organisations on the ethics and legality of adopting facial recognition technology.

We designed the audit based on extensive research as a tool to help:

- Reveal the risks and harms of police use of facial recognition
- Evaluate compliance with the law and national guidance
- Inform policy, advocacy, and ethics scrutiny on police use of facial recognition

Our results

In the summer of 2022, we applied this audit to three facial recognition deployments:

1. ***Bridges* case on South Wales Police's trial of live facial recognition**
   Between 2017 and 2019, South Wales Police conducted operational trial deployments of live facial recognition, which were ruled unlawful in *R (Bridges) v. Chief Constable of South Wales Police.*
2. **Metropolitan Police Service's trial of live facial recognition**
   Between 2016 and 2019, the Metropolitan Police Service conducted ten trial deployments of live facial recognition during policing operations.
3. **South Wales Police's trial of mobile phone facial recognition**
   Between 2021 and 2022, South Wales Police conducted a three-month operational trial of operator initiated facial recognition using a mobile phone application.

We found that all three deployments failed to meet the minimum ethical and legal standards for the governance of facial recognition technology. In this report, we show how these deployments did not incorporate many of the known practices for the safe and ethical use of large-scale data systems.

The reasons for this are as below:

Privacy
The deployments were very broad in scope and may have infringed upon privacy rights. The deployments might not have been ‘in accordance with the law’ or ‘necessary in a democratic society’, as required by human rights law. For example, South Wales Police used live facial recognition at a peaceful protest, interfering with the rights to freedom of expression and assembly.

Discrimination
The deployments were not transparently evaluated for bias in the technology or discrimination in its usage. For example, the Metropolitan Police did not publish an evaluation of the racial or gender bias in the technology before their live facial recognition trials. They also did not publish demographic data on the resulting arrests, making it hard to evaluate if the technology perpetuates racial profiling.

Accountability
The deployments did not ensure that there was a reliable ‘human in the loop’. There were also no clear redress measures for people harmed by the use of facial recognition. Additionally, police force documents were not fully accessible to people with disabilities or provided in immigrant languages, making it difficult for certain groups to understand how the technology impacts them.

Oversight
The deployments lacked regular oversight from an independent ethics committee and the public, especially marginalised communities most affected. For example, the ethics body overseeing South Wales Police’s trials had no independent experts in human rights or data protection based on the available meeting notes. South Wales Police also did not consult the public or civil society for feedback before their trials.

Our recommendations

There have been improvements in how police use facial recognition, but more work needs to be done. Based on this research, we recommend regulators, civil society groups, and researchers to:

A. Use this audit to scrutinise police use of facial recognition

B. Evaluate the use of biometric technologies in other contexts and regions

C. Join calls for a ban on police use of facial recognition in public spaces

What does this audit contribute?

Our audit is unique in that (1) it provides a framework tailored to the specific context of police use of facial recognition in England and Wales and (2) it addresses both legal and ethical standards.

This audit is intended for use in the external scrutiny of police deployments of facial recognition, in order to improve accountability to the public. As a tool for outside stakeholders, this audit complements impact assessments and regulatory guidance aimed for police forces.

Who is this audit for?

We have designed this audit to be administered by outside stakeholders independent of the police in order to provide impartial and meaningful scrutiny. Key stakeholders who we imagine might administer this audit or use the findings include:

A. Regulatory and oversight bodies

B. Policymakers

C. Civil society groups

What is the structure of this audit?

The audit comprises the following four sections, each with a comprehensive set of questions:

1. Legal Standards: Evaluates how police demonstrate their legal compliance for the use of facial recognition. It includes questions about human rights, equality, and data protection.

2. Technical Reliability: Evaluates the reliability of facial recognition and the rigour and transparency of police evaluations. It includes questions about algorithmic bias and robust practice.

3. Human Decision-Making: Evaluates how facial recognition changes police decisions. It includes questions about human review, police training, and accountability.

4. Expertise and Oversight: Evaluates the expertise and oversight over police use of facial recognition. It includes questions about ethics committees and community engagement.

When to use this audit?

This audit can be conducted as an investigation after a police force's facial recognition deployment(s). The audit can also be used to assess a proposed or ongoing use of facial recognition technology, but the results may be limited based on what information is available.

Limitations of this audit

A. This audit does not capture all harms related to the use of facial recognition.

B. This audit may reveal the risks of police use of facial recognition, but is not a substitute for holding the police accountable for its use.

C. Auditor independence is critical for this audit to be meaningful.

D. This audit consists of yes/no questions, which helps make the audit simple to use, and ensures the results are more consistent, although the audit might not capture the complexity of many situations.

We hope that this audit becomes part of larger conversations about whether police should use facial recognition technologies at all. However, given that police forces continue to adopt facial recognition, this audit can help outside stakeholders identify deficiencies and scrutinise the use of the technology. For example, the audit results can point to considerations that have been neglected in the deployment of the technology, such as community oversight, a transparent evaluation of discrimination, or an adequate human rights assessment.

Given the audit's own limitations, performing well on the audit does not green-light the technology's adoption. Rather, the audit can be used to evaluate whether the minimum ethical and legal standards to mitigate harm are met.

SECTION 1

INTRODUCTION

Police use of facial recognition technology (FRT) remains the subject of significant debate around the world.

Police often advocate for the adoption of FRT to help address crime and prevent threats to public security. Facial recognition is considered an important tool for policing that can help identify vulnerable, missing, and wanted individuals.

However, police use of FRT also poses threats to human rights, especially for racialised and marginalised communities. Facial recognition has serious implications for rights such as privacy, equality, and freedom of expression and assembly.

For example, in 2016 and 2017, the London Metropolitan Police Service tested FRT at the Notting Hill Carnival, a Black Caribbean festival in the UK, which resulted in several innocent people being stopped due to misidentifications.[1]

This example illustrates the bias inherent in the technology: FRT has been shown to disproportionately misidentify people of colour, especially dark-skinned women.[2] Moreover, this use of FRT in an area with predominantly people of colour highlights the risk of FRT adoption exacerbating existing disproportionate policing practices.[3]

Given the significant risks of facial recognition, there have been calls for new legislation and bans on police use of the technology. The UK House of Lords Committee on Justice and Home Affairs underscored the urgent need for a stronger legal framework for new technologies in law enforcement, noting the lack of a 'clear line of accountability for the misuse or failure of technological solutions'.[4]

[1] National Physical Laboratory and Metropolitan Police Service, *Metropolitan Police Service Live Facial Recognition Trials: Trials Period August 2016–February 2019* (February 2020) <https://www.met.police.uk/syssiteassets/media/downloads/central/services/accessing-information/facial-recognition/met-evaluation-report.pdf> [accessed 12 July 2022].

[2] Joy Buolamwini and Timnit Gebru, 'Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification', *Proceedings of Machine Learning Research*, 81 (2018), 1–15 <https://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf> [accessed 12 July 2022].

[3] In the year ending March 2021, Black people were seven times more likely to be stopped and searched compared to white people in England and Wales. See: Ethnicity Facts and Figures, 'Stop and Search', *Gov.uk* (27 May 2022) <https://www.ethnicity-facts-figures.service.gov.uk/crime-justice-and-the-law/policing/stop-and-search/latest> [accessed 12 July 2022].

[4] House of Lords, Justice and Home Affairs Committee, *Technology Rules? The Advent of New Technologies in the Justice System*, 1st Report of Session 2021–22, HL Paper, 180 (March 2022) <https://committees.parliament.uk/publications/9453/documents/163029/default/> [accessed 12 July 2022].

The European Parliament and the UN High Commissioner for Human Rights have made calls for the prohibition of the use of FRT in public spaces.[5] Globally, more than 200 civil society organisations have called for a ban on facial recognition in public spaces due to its unmitigable threat of enabling mass surveillance.[6]

Given the ongoing use of facial recognition and its implications for human rights, we need to assess how police are using the technology today.

We propose this sociotechnical audit to help outside stakeholders evaluate the ethics and legality of police use of FRT. Developed for England and Wales, the audit extends to all types of FRT for identification including live, retrospective, and mobile phone FRT.

[5] European Parliament, Committee on Civil Liberties, Justice and Home Affairs, *Report on Artificial Intelligence in Criminal Law and its Use by the Police and Judicial Authorities in Criminal Matters*, 2020/2016(INI) (13 July 2021) <https://www.europarl.europa.eu/doceo/document/A-9-2021-0232_EN.html> [accessed 12 July 2022]; United Nations, Office of the High Commissioner for Human Rights, 'Artificial Intelligence Risks to Privacy Demand Urgent Action – Bachelet', *Press Releases* (15 September 2021) <https://www.ohchr.org/en/2021/09/artificial-intelligence-risks-privacy-demand-urgent-action-bachelet> [accessed 12 July 2022].

[6] Access Now, Amnesty International, European Digital Rights, Human Rights Watch, Internet Freedom Foundation, Instituto Brasileiro de Defesa do Consumidor, and others, 'Open Letter Calling for a Global Ban on Biometric Recognition Technologies that Enable Mass and Discriminatory Surveillance' (21 December 2021) <https://www.accessnow.org/ban-biometric-surveillance/> [accessed 12 July 2022].

We structure this report as follows:

- In **Section 2**, we provide key definitions, background information, and a primer on how FRT works. We also cover related frameworks for assessing the use of FRT.
- In **Section 3**, we address our motivations for this audit, including how we imagine stakeholders can use the audit.
- In **Section 4**, we describe our methodology.
- In **Section 5** we describe the four sections of audit questions on the sociotechnical aspects of police use of FRT: (1) Legal Compliance, (2) Technical Reliability, (3) Human Decision-Making, and (4) Expertise and Oversight.
- In **Section 6**, we present the audit scorecard that can be used to evaluate police use of FRT.
- In **Section 7**, we apply this audit to three facial recognition deployments: (a) *Bridges* case on South Wales Police's trial of live FRT, (b) Metropolitan Police Service's trial of live FRT, and (c) South Wales Police's trial of mobile phone FRT. We find that these deployments fail to meet the minimum ethical and legal standards for the governance of FRT.
- In **Section 8,** we discuss key limitations of the audit. Importantly, the audit does not capture all harms related to police use of facial recognition. Thus, performing well on the audit does not green-light the use of FRT. Rather, this audit can help outside stakeholders assess whether the minimum ethical and legal standards are met in order to scrutinise the use of the technology.
- In **Section 9**, we conclude with recommendations for others, including policymakers, regulators, civil society groups, and researchers, based on the gaps highlighted by our research.

We hope this sociotechnical audit is a step towards revealing and understanding the sociotechnical risks of police use of facial recognition.

The broad range of risks that this report highlights needs scrutiny and discussion if our society is to centre human rights and improve accountability in how technology is used.

SECTION 2

BACKGROUND

2.1 Key definitions

An **audit** is a tool for evaluating the compliance of a system with respect to predefined standards.[7] The audit that we present here evaluates the sociotechnical system of police use of facial recognition technology in England and Wales. The term **sociotechnical** refers to the interactions between people and a technology.

Facial recognition technology (FRT) refers to a digital tool used to perform tasks on images or videos of human faces.[8] This audit extends to all types of FRT used for **identification**, which is also called one-to-many facial recognition. Here, a facial image or probe image is first captured and then compared with a database or watchlist that contains known facial images in order to determine if there is a match. See **Section 2.2** for further details on how facial recognition works.

Our audit evaluates police use of FRT with respect to legal and ethical standards. **Legality** is defined as compliance with the law in England and Wales. Currently, there is no explicit legal basis and primary legislation for police use of FRT in the UK. Thus, legal standards in the audit are primarily informed by the Human Rights Act 1998, the Equality Act 2010, and the Data Protection Act 2018, which are relevant to the governance of facial recognition as the technology interferes with rights protected by these acts.

The term **ethics** encapsulates the principles of fairness, transparency, and accountability. In the context of this work, **fairness** refers to the elimination of the discriminatory effects of police use of FRT on individuals and groups. **Transparency** refers to the quality of police being open about their use of FRT in a complete, understandable, and accessible manner. **Accountability** refers to the state of the police being responsible or answerable to the public for the societal impacts of their use of FRT.

[7] Ada Lovelace Institute and DataKind UK, 'Examining the Black Box: Tools for Assessing Algorithmic Systems, Identifying Common Language for Algorithm Audits and Impact Assessments' (29 April 2020) <https://www.adalovelaceinstitute.org/report/examining-the-black-box-tools-for-assessing-algorithmic-systems/> [accessed 12 July 2022].

[8] Joy Buolamwini, Vincente Ordóñez, Jamie Morgenstern, and Erik Learned-Miller, *Facial Recognition Technologies: A Primer* (29 May 2020) <https://assets.website-files.com/5e027ca188c99e3515b404b7/5ed1002058516c11edc66a14_FRTsPrimerMay2020.pdf> [accessed 12 July 2022].

2.2 Primer on facial recognition

Our audit extends to all types of FRT used for identification. Here, we explain how FRT for identification works and how the performance of FRT can be measured. We also discuss how the *false positive rate* can give a misleading impression of good performance and highlight the importance of reporting the *precision* of FRT.

Facial recognition for identification: First, a facial image or *probe image* of an individual is captured. The probe image could be captured using surveillance camera footage, a mobile phone, or even social media. Using FRT, this probe image is searched against a database or *watchlist* of known facial images in order to determine if there is a *match*. In the context of policing, the watchlist might include arrested or missing persons. **Figure 1** shows this process. Facial recognition for identification is also referred to as one-to-many facial recognition, since the probe image is compared with not just a single image but a set of images in the watchlist.[9]

Note that in practice the probe image and watchlist images are not directly compared. Rather, the FRT algorithm generates a corresponding biometric template for each image. FRT then compares these templates, which are digital representations of the images.

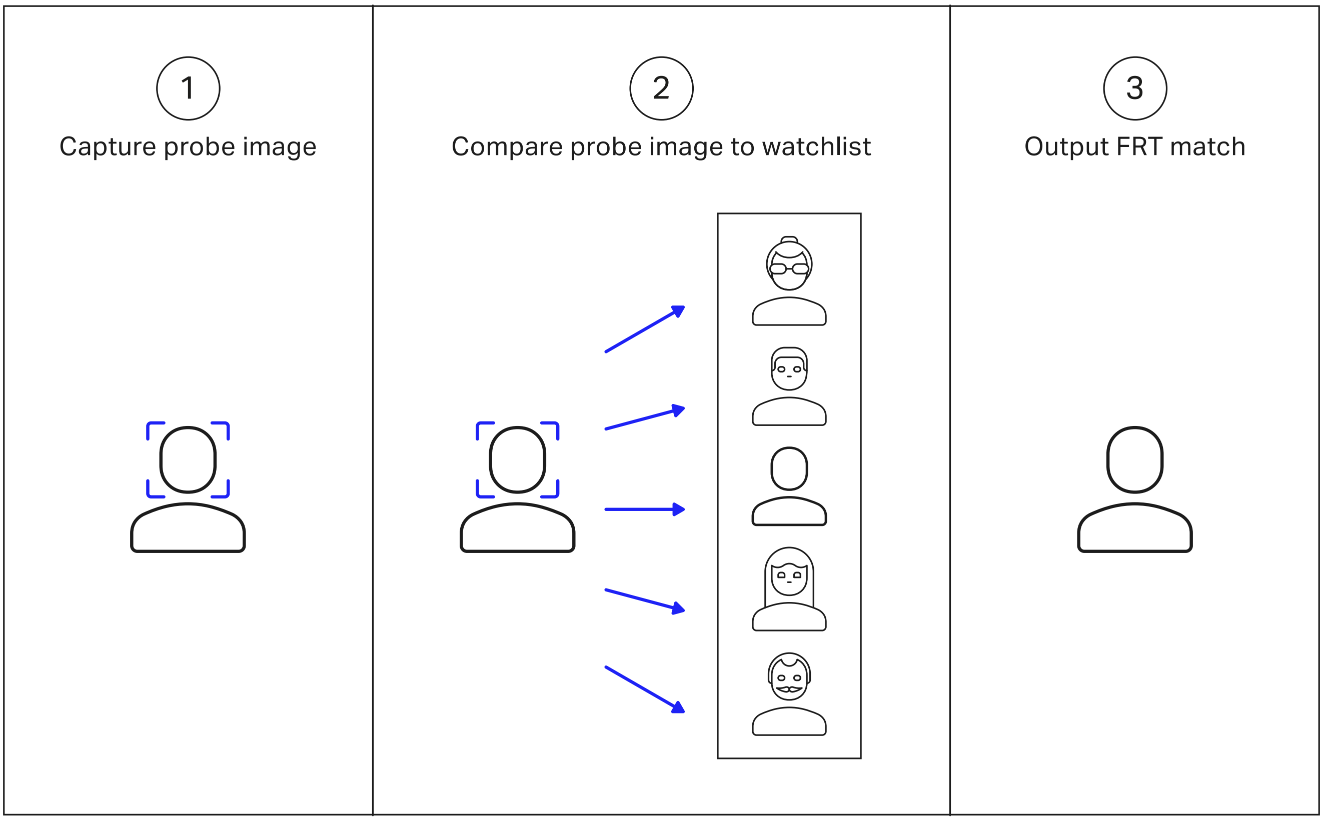


Figure 1: The process of using facial recognition for identification, or one-to-many facial recognition. First, a probe image of a person is captured. Then, the probe image is compared with a watchlist of known facial images to determine if there is a match.

[9] Joy Buolamwini, Vicente Ordóñez, Jamie Morgenstern, and Erik Learned-Miller, *Facial Recognition Technologies: A Primer* (29 May 2020) <https://assets.website-files.com/5e027ca188c99e3515b404b7/5ed1002058516c11edc66a14_FRTsPrimerMay2020.pdf> [accessed 12 July 2022].

Types of facial recognition: There are different types of FRT used for identification. Live facial recognition (LFR) refers to FRT where images, such as from a live camera feed, are compared to the watchlist in real time. Retrospective facial recognition (RFR) refers to FRT where images, such as from surveillance camera footage, are compared to the watchlist at a later point in time. Mobile phone or operator initiated facial recognition (OIFR) refers to FRT where images captured using a mobile phone are compared to the watchlist in near real time. **Table 1** summarises these different types of facial recognition.

Facial Recognition Type	Image Capture From...	Image Identification
Live Facial Recognition	A van/street surveillance camera	In real time
Retrospective Facial Recognition	A van/street surveillance camera or social media	At a later point in time
Operator Initiated Facial Recognition	A mobile phone camera	In near real time

Table 1: Summary of the different types of facial recognition.

Performance of facial recognition: In this section, we discuss how the performance of a facial recognition system can be measured in the context of its operational use by police. Refer to **Figure 2** for a visualisation of the performance metrics that we discuss.

When an individual is scanned using FRT, their probe image is searched against a watchlist using FRT. There are two cases when the FRT system outputs a negative result and does not produce a match (any grey icon):

1. *True negative:* FRT correctly outputs that an individual is not on the watchlist (empty grey icon).

2. *False negative:* FRT incorrectly outputs that an individual is not on the watchlist, meaning that the FRT system missed a correct match (lilac-filled grey icon).

Alternatively, the FRT system may output a positive result and produce a match (any black icon). In this case, police officers review the FRT matches to bring a 'human in the loop'. Officer-verified matches are the matches deemed correct by officers (any black icon with blue box). If there is no engagement with the person for an officer-verified match (empty black icon with blue box), then it is uncertain whether this match is actually correct since officers may have made a misidentification. If there is an engagement with the person for an officer-verified match, then there are two possibilities:

1. *True positive:* An officer-verified match is confirmed to be correct (lilac-filled black icon with blue box).

2. *False positive:* An officer-verified match is confirmed to be incorrect (red-filled black icon with blue box).

Next, we discuss common metrics to measure the performance of a facial recognition system. Using multiple metrics is important, as no single metric fully captures the accuracy of an FRT system.

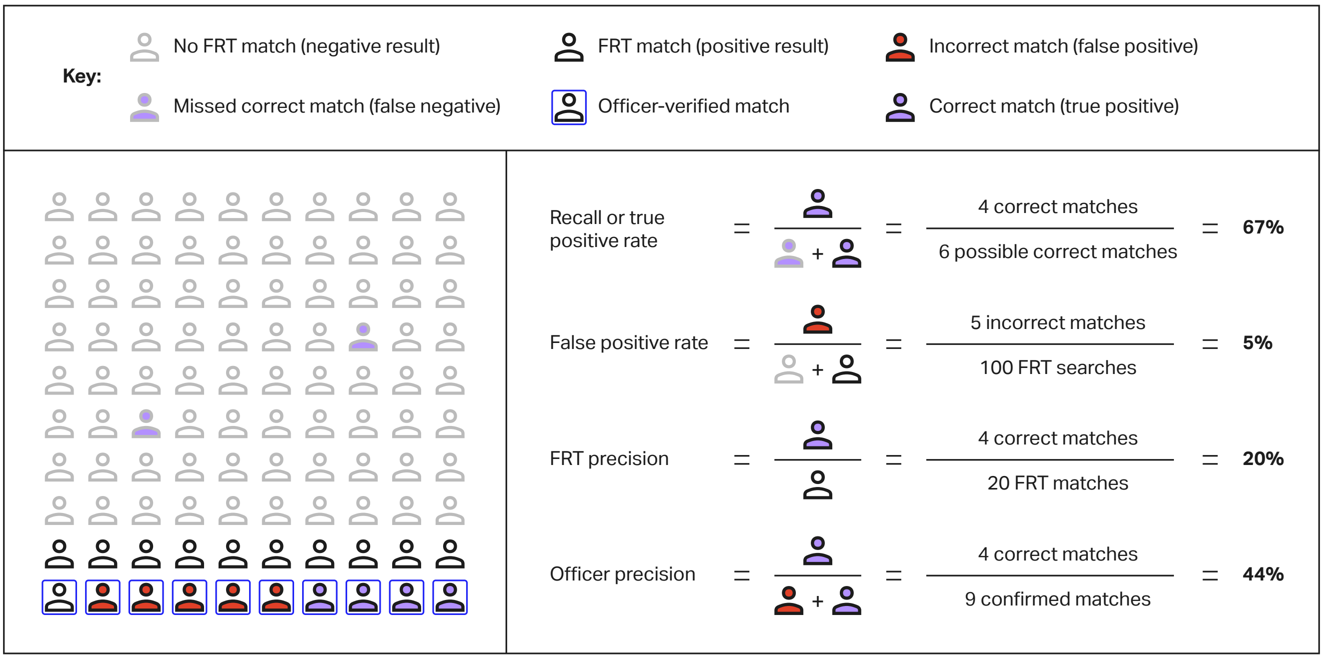

Key:
No FRT match (negative result)
Missed correct match (false negative)
FRT match (positive result)
Officer-verified match
Incorrect match (false positive)
Correct match (true positive)
Recall or true positive rate
4 correct matches
6 possible correct matches
67%
False positive rate
5 incorrect matches
100 FRT searches
5%
FRT precision
4 correct matches
20 FRT matches
20%
Officer precision
4 correct matches
9 confirmed matches
44%

Figure 2: Summary of performance metrics for facial recognition in the context of policing.

A. *True positive rate* captures: What percentage of people on the watchlist who are scanned using FRT produce a correct match? Specifically, this metric is the number of confirmed correct matches, as a proportion of the total possible correct matches.[10]

B. *False positive rate* captures: What percentage of total people who are scanned using FRT produce an incorrect match? Specifically, this metric is the number of confirmed incorrect matches, as a proportion of the total people who are scanned using FRT.[11]

C. *FRT precision* captures: What percentage of FRT matches are correct? Specifically, this metric is the number of confirmed correct matches, as a proportion of the total matches produced by the FRT system.

D. *Officer precision* captures: What percentage of confirmed matches are correct? Specifically, this metric is the number of confirmed correct matches, as a proportion of the total FRT matches that are confirmed to be either correct or incorrect.

We note that when FRT is used operationally, the true positive rate can only be calculated if a watchlist of known persons is used to monitor the performance.[12] Without such a watchlist, the identities of individuals who produce no FRT match are unknown, making it impossible to calculate the number of missed correct matches. However, if FRT is applied to the known persons on such a watchlist, the number of missed correct matches and thus the true positive rate can be calculated.

[10] True positive rate is also referred to as recall.

[11] This definition of false positive rate slightly differs from the conventional definition in mathematics. Using the conventional definition, the false positive rate would be the number of confirmed incorrect matches, as a proportion of the total number of people scanned who are not on the watchlist. However, in our definition, the total number of people scanned who are not on the watchlist is estimated simply as the total number of people who are scanned, since the former metric is unknown in an operational setting. We have seen this done in practice by the College of Policing and police forces in the UK.

[12] College of Policing, ‘Terminology’, *Authorised Professional Practice* (22 March 2022) <https://www.college.police.uk/print/pdf/node/3005> [accessed 12 July 2022].

False positive rate vs. precision: Police forces often use the false positive rate to assess the performance of FRT.[13] However, reporting only the false positive rate can give a misleading impression of good performance.

The false positive rate compares with the total people scanned using FRT, which results in a very low false positive rate if a large number of people are scanned (see **Figure 3**). For example, if police deploy facial recognition, either live or retrospectively, in a public space where there is a large crowd, the number of people scanned would likely range from 1,000 to 20,000.

However, the majority of these people are expected to not be on the watchlist.[14] Therefore, there would be few FRT matches and also few incorrect matches, compared to the large number of people scanned, resulting in a low false positive rate.

This low false positive rate is expected due to the nature of the crowd and does not necessarily imply that FRT performs well. For example, most of the FRT matches might be incorrect, indicating that FRT does not perform well (see **Figure 3**).

Thus, it is critical to report the precision of FRT when assessing performance. Instead of comparing with the total people scanned, the precision compares with the number of FRT matches and measures the proportion of these that is correct.

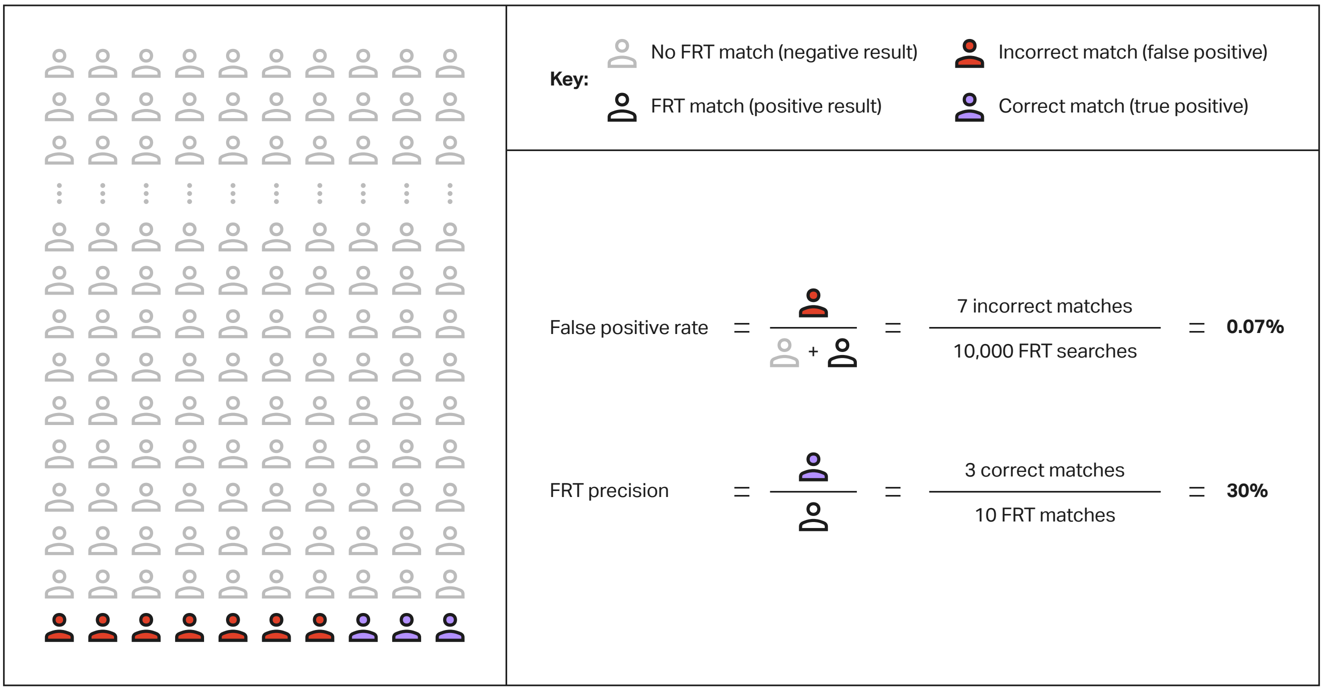


Figure 3: Distinction between the false positive rate and precision of facial recognition.

[13] South Wales Police, 'List of Previous FRT Deployments' <https://www.south-wales.police.uk/SysSiteAssets/media/downloads/south-wales/about-us/frt/FRT-deployments.pdf> [accessed 12 July 2022].

[14] The watchlist likely comprises criminal suspects. The majority of the public is expected to not be a criminal suspect, and thus expected to not be on the watchlist.

2.3 UK police use of facial recognition

In England and Wales, police forces have increasingly developed and deployed facial recognition. More than 10 forces have used FRT, with South Wales Police and the Metropolitan Police Service notably having deployed live FRT. Since September 2019, all police forces have had access to retrospective FRT through the Police National Database, although there is limited information about how the technology is being used.[15]

Even though the majority of FRT deployments are trials, facial recognition has been used operationally for policing purposes during trials. Moreover, the use of FRT has not been very centralised, and different forces have deployed the technology using different standards. **Appendix A** includes a full list of police forces in England and Wales that are known to have used FRT.

Many police forces advocate for the use of FRT to help fulfil their operational responsibilities to prevent and detect crime, bring offenders to justice, and protect against threats to public security.[16] Police forces often consider facial recognition an important aspect of policing that can help identify vulnerable, missing, and wanted individuals, especially known serious offenders.[17]

[15] Home Office News Team, 'Fact Sheet on Live Facial Recognition Used by Police' (4 September 2019) <https://homeofficemedia.blog.gov.uk/2019/09/04/fact-sheet-on-live-facial-recognition-used-by-police/> [accessed 12 July 2022]; Will Grimond and Asheem Singh, *A Force for Good? Results from FOI Requests on Artificial Intelligence in the Police Force* (RSA, April 2020) <https://www.thersa.org/globalassets/reports/2020/a-force-for-good-police-ai.pdf> [accessed 12 July 2022].

[16] Metropolitan Police Service, 'Live Facial Recognition: Legal Mandate' (29 November 2022) <https://www.met.police.uk/SysSiteAssets/media/downloads/force-content/met/advice/lfr/policy-documents/lfr-legal-mandate.pdf> [accessed 12 July 2022].

[17] South Wales Police, 'New Facial Recognition Mobile App to Identify Vulnerable, Missing and Wanted Individuals' (7 December 2021) <https://www.south-wales.police.uk/news/south-wales/news/2021/december/new-facial-recognition-app-to-to-identify-wanted-individuals/> [accessed 12 July 2022].

Police officers often feel under-resourced, overburdened, and under pressure to cover gaps in other services, for example, for mental health support.[18] Thus, FRT is viewed as a tool that can help officers carry out their duties by locating persons of interest quickly and cost efficiently.

Police forces often highlight examples of using FRT to fight terrorism and serious crime: the technology can be used to identify persons of interest for terrorism reasons at borders, support the investigation of knife crime, or find missing persons believed to be at risk of child sexual abuse.

We note that the current and potential use of FRT extends beyond these cases. For example, the technology may be used to identify victims, potential witnesses, or persons with mental health issues.[19] This broad scope of FRT usage has raised serious concerns of the technology interfering with the rights of innocent people and marginalised communities.

With the increasing number of deployments of FRT in the UK, there have been growing debates about the legitimacy of police use of this technology. The adoption of facial recognition has been critiqued for posing threats to civil liberties.

For example, the Court of Appeal in *R (Bridges) v. Chief Constable of South Wales Police* found that South Wales Police's use of live FRT did not comply with human rights, equality, and data protection law. An independent review of the Metropolitan Police Service's trial of live FRT concluded that the police force had an insufficient legal basis and conducted an inadequate assessment of human rights.[20] In the next subsection, we discuss the risks that arise from police use of FRT in more detail.

[18] Vikram Dodd, 'Police Resources "Drained to Dangerously Low Levels", Say Former Top Officers', *The Guardian* (5 July 2019) <https://www.theguardian.com/uk-news/2019/jul/04/police-watchdog-reforms-chief-inspector-constabulary> [accessed 12 July 2022]; Winchester, Nicole, 'Covid-19 and the Police: New Powers but More Pressure?', *House of Lords Library*, In Focus (27 March 2020) <https://lordslibrary.parliament.uk/covid-19-and-the-police-new-powers-but-more-pressure/> [accessed 12 July 2022].

[19] College of Policing, 'Watchlist', Authorised Professional Practice (22 March 2022) <https://www.college.police.uk/print/pdf/node/3002> [accessed 12 July 2022]; Mark Townsend, 'Police to Use Facial-Recognition Cameras at Cenotaph Service', *The Observer* (12 November 2017) <https://www.theguardian.com/technology/2017/nov/12/metropolitan-police-to-use-facial-recognition-technology-remembrance-sunday-cenotaph> [accessed 12 July 2022]; Fraser Sampson, 'The Biometrics and Surveillance Cameras Commissioner's Response to the College of Policing APP on Live Facial Recognition', *Gov.uk* (6 April 2022) <https://www.gov.uk/government/news/the-biometrics-and-surveillance-camera-commissioners-response-to-the-college-of-policing-app-on-live-facial-recognition> [accessed 12 July 2022].

[20] Pete Fussey, and Daragh Murray, *Independent Report on the London Metropolitan Police Service's Trial of Live Facial Recognition Technology*, The Human Rights, Big Data and Technology Project (University of Essex, July 2019) <http://repository.essex.ac.uk/24946/1/London-Met-Police-Trial-of-Facial-Recognition-Tech-Report-2.pdf> [accessed 12 July 2022].

2.4 Harms of police use of facial recognition

Police use of facial recognition technology can pose serious threats to fundamental rights of privacy, freedom of expression and assembly, and freedom from discrimination. Additional ethical concerns arise as police procure the technology from private vendors. Below we discuss these harms and how they often disproportionately fall on marginalised communities.

Privacy and data protection: FRT interferes with the rights to privacy and data protection. The technology involves scanning and identifying people from their facial images, and the potential retention of these images, often without their knowledge or consent. Through this use and collection of personal data, FRT can pose a serious threat to the privacy and data protection rights, for example, of every person who is scanned using FRT. In the UK, these rights are codified in the Data Protection Act 2018 and the Human Rights Act 1998 (Article 8).

Freedom of expression and assembly: The use of FRT for surveillance can inhibit our ability to express ideas and engage in democratic processes.[21] FRT adoption can generate a 'chilling effect' where individuals withhold from exercising their fundamental rights, such as the right to protest, because of a fear of the consequences.[22] For example, individuals may decide not to attend public gatherings or partake in protests. The rights to freedom of expression and assembly are crucial in a democratic society, and the impact of FRT on them will be considerable if FRT is integrated into body worn cameras or CCTV networks. In the UK, these rights are codified in the Human Rights Act 1998 (Article 10 and Article 11).

[21] Liberty, 'Briefing on the Amended Surveillance Camera Code of Practice' (January 2022) <https://www.libertyhumanrights.org.uk/wp-content/uploads/2022/01/Libertys-briefing-on-the-amended-Surveillance-Camera-Code-of-Practice-January-2022.pdf> [accessed 12 July 2022].

[22] Fussey and Murray, *Independent Report*. p. 36.

Equality and non-discrimination: The use of facial recognition also raises serious discrimination concerns. In the UK, the prohibition of discrimination is protected under the Equality Act 2010 and the Human Rights Act 1998 (Article 14).

One key issue is the discriminatory use of the technology. Historically, surveillance systems have been used to monitor marginalised groups.[23] Police use of FRT could perpetuate existing disproportionate policing practices such as stop and search that often target people of colour and low-income communities.[24] In the year ending March 2021, Black people were seven times more likely to be stopped and searched compared to white people in England and Wales.[25] Many people are concerned that FRT will exacerbate racial profiling and discrimination already prevalent in policing.[26]

Another discrimination issue is the inherent bias in the technology. Studies have shown that FRT disproportionately misidentifies women, people of colour, and people with disabilities.[27] An incorrect identification can lead to disproportionate police interventions with innocent members of these communities, where individuals are questioned and subject to unwarranted intrusions (e.g. their images retained, their fingerprints scanned, subjected to stop and search, and wrongful arrest).

While reducing the inherent bias in the technology may mitigate some harms, it does not eliminate the technology's discriminatory use and its impact on other rights. In fact, improving the technology's performance might perfect it as a tool of mass surveillance.

[23] Simone Browne, *Dark Matters: On the Surveillance of Blackness* (Durham: Duke University Press, 2015); Ruha Benjamin, *Race After Technology: Abolitionist Tools for the New Jim Code* (Cambridge: Polity, 2019).

[24] Liberty, 'Briefing on the Amended Surveillance Camera Code of Practice'.

[25] Ethnicity Facts and Figures, 'Stop and Search'.

[26] Patrick Williams, *Being Matrixed: The (Over)Policing of Gang Suspects in London* (StopWatch, August 2018) <https://www.stop-watch.org/what-we-do/research/being-matrixed-the-overpolicing-of-gang-suspects-in-london/> [accessed 12 July 2022]; Danielle Dwyer, Wesley Johnson, with PA, 'Police Apologise over CCTV in Muslim Areas', *The Independent* (30 September 2010) <https://www.independent.co.uk/news/uk/crime/police-apologise-over-cctv-in-muslim-areas-2094167.html> [accessed 12 July 2022]; BBC News, 'Black Police Leader Says Some Forces "Still Institutionally Racist"' (17 January 2018) <https://www.bbc.co.uk/news/uk-england-42702432> [accessed 12 July 2022].

[27] Buolamwini and Gebru, 'Gender Shades'; Sheri Byrne-Haber, 'Disability and AI Bias', *Medium* (11 July 2019) <https://sheribyrnehaber.medium.com/disability-and-ai-bias-cced271bd533> [accessed 12 July 2022].

Public-private collaboration: Police forces often develop and deploy facial recognition in collaboration with private vendors. These collaborations can exacerbate issues of bias, especially if the police do not scrutinise the vendor's technology, and issues of privacy, as data may be repurposed and shared more broadly.[28]

Moreover, police can perpetuate harm indirectly if they acquire or procure technology from vendors involved in unethical practices. Examples of documented unethical practices include IBM using photos of individuals without their consent to improve their FRT, and the involvement of Hikvision's CCTV cameras in the persecution of Uighur Muslims in China.[29]

[28] Biometrics and Forensics Ethics Group, *Briefing Note on the Ethical Issues Arising from Public-Private Collaboration in the Use of Live Facial Recognition Technology* (January 2021) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/953359/LFR_briefing_note_18.1.21.final.pdf> [accessed 12 July 2022], pp. 5–6.

[29] Olivia Solon, 'Facial Recognition's "Dirty Little Secret": Millions of Online Photos Scrapes Without Consent', NBC News (17 March 2019) <https://www.nbcnews.com/tech/internet/facial-recognition-s-dirty-little-secret-millions-online-photos-scraped-n981921> [accessed 12 July 2022]; House of Commons, Foreign Affairs Committee, *Never Again: The UK's Responsibility to Act on Atrocities in Xinjiang and Beyond*, 2nd Report of Session 2021–22, HC, 198 (8 July 2021) <https://committees.parliament.uk/publications/6624/documents/71430/default/> [accessed 12 July 2022]; Fraser Sampson, 'Letter from the Biometrics and Surveillance Camera Commissioner to the Secretary of State for Levelling Up, Housing and Communities', *Gov.uk* (22 April 2022) <https://www.gov.uk/government/publications/letters-from-the-biometrics-and-surveillance-camera-commissioner-april-2022/letter-from-the-biometrics-and-surveillance-camera-commissioner-to-the-secretary-of-state-for-levelling-up-housing-and-communities-22-april-2022-acc> [accessed 12 July 2022]; *Big Brother Watch UK, Who's Watching You? The Dominance of Chinese-State Owned CCTV in the UK* (7 February 2022) <https://bigbrotherwatch.org.uk/wp-content/uploads/2022/02/Whos-Watching-You_The-dominance-of-Chinese-state-owned-CCTV-in-the-UK.pdf> [accessed 12 July 2022].

Criminal justice system: Historically, there have been issues of over-policing and disproportionate incarceration of marginalised communities in the UK criminal justice system that continue today.[30] Numerous investigations have shown the prevalence of misogyny and racism in the culture of British policing.[31] The recently passed Policing and Crime Sentencing and Courts Bill has been criticised for restricting the right to protest, discriminating against the Traveller community, and exacerbating racism in policing.[32]

While surveillance systems such as facial recognition are often justified as tools that improve security, they often threaten the safety of people of colour and other marginalised communities.[33] Instead of using FRT surveillance to address crime, many advocate for a model of social and transformative justice, where we address underlying inequities and invest in education, healthcare, housing, and community welfare.[34]

[30] David Lammy, *The Lammy Review Final Report: An Independent Review into the Treatment of, and Outcomes for, Black, Asian and Minority Ethnic Individuals in the Criminal Justice System* (8 September 2017) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/643001/lammy-review-final-report.pdf> [accessed 12 July 2022]; Paul Lewis, Tim Newburn, Matthew Taylor, Catriona Mcgillivray, Aster Greenhill, Harold Frayman, and Rob Proctor, *Reading the Riots: Investigating England's Summer of Disorder* (London: London School of Economics and Political Science and *The Guardian*, 2011) <http://eprints.lse.ac.uk/46297/1/Reading%20the%20riots(published).pdf> [accessed 12 July 2022]; Tony Jefferson, 'Policing the Riots: From Bristol and Brixton to Tottenham, via Toxteth, Handsworth, etc.', *Criminal Justice Matters*, 87 (2012), 8–9 <https://doi.org/10.1080/09627251.2012.670995>; Independent Office for Police Conduct, *Operation Hotton, Learning Report* (1 February 2022) <https://www.policeconduct.gov.uk/sites/default/files/Operation%20Hotton%20Learning%20report%20-%20January%202022.pdf> [accessed 12 July 2022]; Amnesty International, *Trapped in the Matrix: Secrecy, Stigma, and Bias in the Mat's Gangs Database* (May 2018) <https://www.amnesty.org.uk/files/reports/Trapped%20in%20the%20Matrix%20Amnesty%20report.pdf> [accessed 12 July 2022].

[31] Joe Ryan, 'Reports of Misogyny and Sexual Harassment in the Metropolitan Police', *House of Commons Library Debate Pack*, CDP 2022/0046 (1 March 2022) <https://researchbriefings.files.parliament.uk/documents/CDP-2022-0046/CDP-2022-0046.pdf> [accessed 12 July 2022]; Amnesty International, *Trapped in the Matrix*.

[32] Amnesty International, 'UK: Dark Day for Civil Liberties as "Deeply-Authoritarian" Policing Bill Passed by Lords' (27 April 2022) <https://www.amnesty.org.uk/press-releases/uk-dark-day-civil-liberties-deeply-authoritarian-policing-bill-passed-lords> [accessed 12 July].

[33] Tamika Lewis, Seeta Peña Gangadharan, Mariella Saba, and Tawana Petty, *Digital Defense Playbook: Community Power Tools for Reclaiming Data* (Detroit: Our Data Bodies, 2018) <https://www.odbproject.org/wp-content/uploads/2019/03/ODB_DDP_HighRes_Spreads.pdf> [accessed 12 July 2022].

[34] Angela Yvonne Davis, Are Prisons Obsolete?, Open Media Book (New York: Seven Stories Press, 2003); Alex S. Vitale, The End of Policing (London: Verso, 2017); Cradle Community, *Brick by Brick: How We Build a World Without Prisons* (London: Hajar, 2021); Benjamin, *Race After Technology*, Chapter 5.

2.5 Regulatory gap for UK police use of facial recognition

Globally, there have been calls for legislation on police use of facial recognition. Government bodies, civil society organisations, and researchers have highlighted the existing regulatory gap and the need for a legal framework to govern use of new technologies such as facial recognition. Below, we discuss this in the context of the UK.

Limitations of the Courts: In August 2020, the Court of Appeal in *R (Bridges) v. Chief Constable of South Wales Police* ruled that South Wales Police's use of live facial recognition was unlawful. The Court held that there were 'fundamental deficiencies' in the existing legal framework and identified key gaps in the police force's compliance with human rights, equality, and data protection laws.[35]

However, judicial reviews are limited to the case being brought forth. Scholars suggest that the *Bridges* case leaves significant room for police to continue their use of FRT with only minor, gradual changes.[36] Moreover, as the House of Lords Committee on Justice and Home Affairs highlights, the Courts cannot legislate: 'While they play an essential role in addressing breaches of the law, we cannot expect the Courts to set the framework for the deployment of new technologies.'[37]

Lack of an explicit legal basis: Currently, there is no explicit legal basis for the use of FRT by police in the UK. Civil society, researchers, and the former and current UK Biometrics Commissioner have highlighted the need for parliamentary debate and primary legislation on police use of FRT.[38]

While police common law powers have been used to provide a legal basis, these powers are arguably too vague and can lead to arbitrariness.[39] There is growing consensus that a new legal framework for the use of FRT and other biometric technologies is needed.

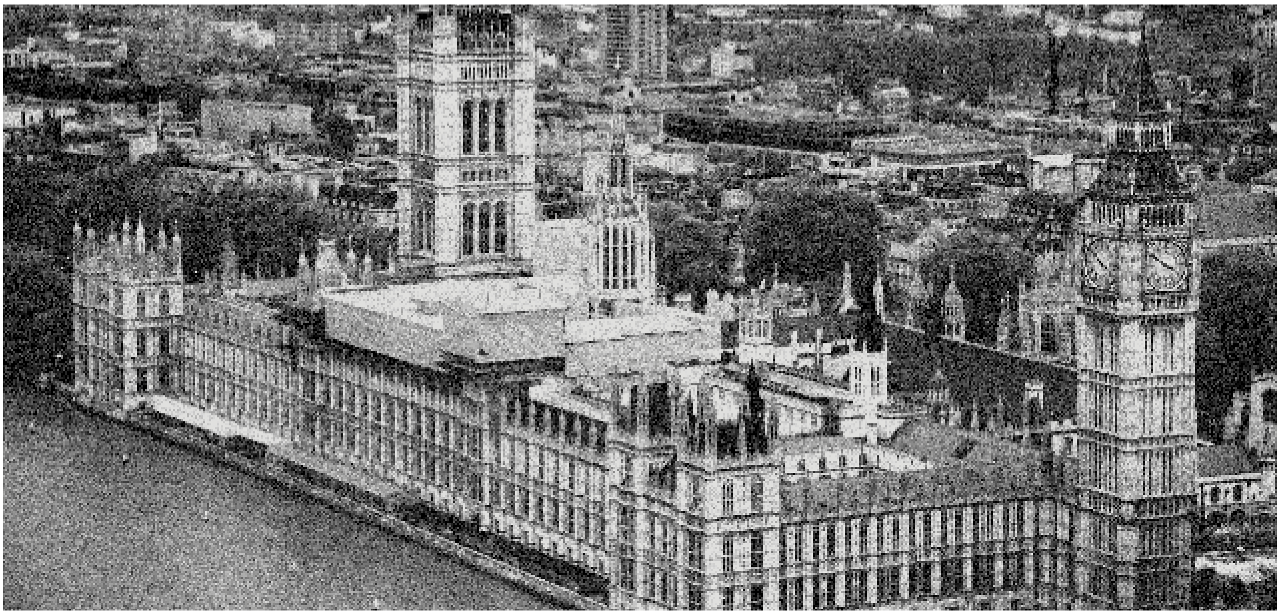
[35] *R (Bridges) v. Chief Constable of South Wales Police*, Judgement, Court of Appeal, Civil Division, case C1/2019/2670 (11 August 2020) <https://www.judiciary.uk/wp-content/uploads/2020/08/R-Bridges-v-CC-South-Wales-ors-Judgment.pdf> [accessed 13 July 2022], para. 91.

[36] Joe Purshouse and Liz Campbell, 'Automated Facial Recognition and Policing: A Bridge Too Far?', *Legal Studies*, 42.2 (2022), 209–227 <https://doi.org/10.1017/lst.2021.22>.

[37] House of Lords, Justice and Home Affairs Committee, *Technology Rules?*, p. 27.

[38] Privacy International, Liberty, Defend Digital Me, Open Rights Group, and Big Brother Watch, 'Consultation on Live Facial Recognition APP. Feedback Form' (27 June 2021) <https://privacyinternational.org/sites/default/files/2021-06/LFRT%20Consultation%20Response%20Final_0.pdf> [accessed 12 July 2022]; Paul Wiles, 'Biometrics Commissioner on the Police Use of Live Facial Recognition', *Gov.uk* (11 February 2020) <https://www.gov.uk/government/news/biometrics-commissioner-on-the-police-use-of-live-facial-recognition> [accessed 12 July 2022]; Fraser Sampson, 'The Biometrics and Surveillance Cameras Commissioner's Response to the College of Policing APP on Live Facial Recognition'.

[39] Matthew Ryder, *The Ryder Review: Independent Legal Review of the Governance of Biometric Data in England and Wales* (Ada Lovelace Institute, June 2022) <https://www.adalovelaceinstitute.org/wp-content/uploads/2022/06/The-Ryder-Review-Independent-legal-review-of-the-governance-of-biometric-data-in-England-and-Wales-Ada-Lovelace-Institute-June-2022.pdf> [accessed 12 July 2022]; Lorna Woods, 'United Kingdom – Automated Facial Recognition in the UK: The *Bridges* Case and Beyond', *European Data Protection Law Review*, 6.3 (2020), 455–463 <https://doi.org/10.21552/edpl/2020/3/16>; Fussey and Murray, *Independent Report*; Privacy International and others, 'Consultation on Live Facial Recognition APP. Feedback Form'.



Need for new legislation: In March 2022, the House of Lords Committee on Justice and Home Affairs called for a stronger legal framework for new technologies in law enforcement, noting the lack of a 'clear line of accountability for the misuse or failure of technological solutions used in the application of the law'.[40] The Ada Lovelace Institute commissioned the 'Ryder Review', an independent legal review of the governance of biometric data in England and Wales, which found that the existing legal framework is not fit for purpose and fails to clarify when and how biometrics can be used.[41]

The current legal framework relies on a patchwork of overlapping legislation focused on human rights, equality, data protection, and criminal justice issues.[42] With different bodies of law being relevant, there is confusion about what legislation applies and who has oversight over decision-making.[43] Moreover, existing legislation is incomplete and fails to consider the specific risks posed by biometrics, especially with regard to collective harms and public-private collaborations.[44]

While there have been efforts to provide guidance, for example through the Surveillance Camera Code of Practice (COP) and the College of Policing's Authorised Professional Practice on live FRT, many argue that these do not provide sufficient governance on the use of FRT. For instance, members of the House of Lords argued that the COP does not constitute a legitimate ethical or legal framework for police use of FRT and is incompatible with human rights requirements.[45]

[40] House of Lords, Justice and Home Affairs Committee, *Technology Rules?*, p. 37.

[41] Ryder, *The Ryder Review*, p. 11.

[42] Relevant legislation includes the Human Rights Act 1998, Equality Act 2010, Data Protection Act 2018, UK General Data Protection Regulation, Police and Criminal Evidence Act 1984, Protection of Freedoms Act 2012, Regulation of Investigatory Powers Act 2000, and Freedom of Information Act 2000.

[43] House of Lords, Justice and Home Affairs Committee, *Technology Rules?*, pp. 25, 27.

[44] Ryder, *The Ryder Review*, pp. 65, 76.

[45] HL Deb, 2 February 2022, c983 <https://www.theyworkforyou.com/lords/?id=2022-02-02a.983.0> [accessed 13 July 2022].

Calls for a ban or moratorium: The European Parliament, the UN High Commissioner for Human Rights, and numerous UK politicians have made calls to prohibit the use of FRT in public spaces, highlighting its risk to privacy, non-discrimination, and freedom of expression and assembly.[46] The Scottish Parliament's Justice Sub-Committee on Policing concluded that 'live facial recognition technology is currently not fit for use by Police Scotland'.[47] The Ryder Review also recommends a moratorium on the use of live facial recognition until a sufficient legal framework is introduced.[48]

Globally, more than 200 civil society organisations have called for a ban on FRT and other biometric technologies in public spaces due to their unmitigable threat of enabling mass surveillance.[49] These groups argue that no technical or legal safeguards could eliminate the threat that FRT poses. In the UK, organisations including Big Brother Watch, Liberty, and Privacy International have led similar campaigns for a ban.

Current bans and moratoriums: In October 2019, the Automated Facial Recognition Technology Bill was introduced in the UK with the aim of prohibiting the use of FRT in public places.[50] However, this UK bill will not make further progress since the Parliament session was discontinued.

In the United States, there have been city-level and state-level bans on police use of FRT, for example, in Boston, Oakland, Portland, San Francisco, Illinois, and Virginia. Illinois' Biometric Information Privacy Act is one of the most far-reaching laws in the U.S. that governs the use of biometric data. Outside of the United States, Belgium, Luxembourg, and Morocco have also introduced prohibitions on facial recognition.[51] However, these bans might expire or be rolled back in the near future, as has already happened for a couple of cases.[52]

[46] European Parliament, Committee on Civil Liberties, Justice and Home Affairs, *Report on Artificial Intelligence in Criminal Law*; United Nations, Office of the High Commissioner for Human Rights, 'Artificial In-telligence Risks to Privacy'; Big Brother Watch UK, 'Joint Statement on Police and Private Company Use of Faci-al Recognition Surveillance in the UK' (September 2019) <https://bigbrotherwatch.org.uk/wp-content/uploads/2019/09/Statement-to-stop-live-facial-recognition-surveillance-BBW-September-2019-1.pdf> [ac-cessed 13 July 2022].

[47] Scottish Parliament, Justice Sub-Committee on Policing, *Facial Recognition: How Policing in Scotland Makes Use of This Technology*, 1st Report, 2020 (Session 5), SP, 678 (11 February 2020) <https://sp-bpr-en-prod-cdnep.azureedge.net/published/JSP/2020/2/11/Facial-recognition--how-policing-in-Scotland-makes-use-of-this-technology/JSPS0520R01.pdf> [accessed 13 July 2022], p. 43.

[48] Ryder, *The Ryder Review*, pp. 78–80.

[49] Access Now and others, 'Open Letter Calling for a Global Ban on Biometric Recognition Technologies'; Big Brother Watch UK, *Stop Facial Recognition* <https://bigbrotherwatch.org.uk/campaigns/stop-facial-recognition/> [accessed 13 July 2022].

[50] *Automated Facial Recognition Technology (Moratorium and Review)*, HL Bill 87, 2019–21 (London: HMSO, 2020) <https://bills.parliament.uk/bills/2610> [accessed 13 July 2022].

[51] Paul Bischoff, 'Facial Recognition Technology (FRT): 100 Countries Analyzed' (8 June 2021) <https://www.comparitech.com/blog/vpn-privacy/facial-recognition-statistics/> [accessed 13 July 2022].

[52] Paresh Dave, 'U.S. Cities Are Backing Off Banning Facial Recognition as Crime Rises' (12 May 2022) <https://www.reuters.com/world/us/us-cities-are-backing-off-banning-facial-recognition-crime-rises-2022-05-12/> [accessed 13 July]; Chris Burt, 'Morocco Extends Facial Recognition Moratorium to Year-End, Proposes Biometric Authentication Service' (9 April 2020) <https://www.biometricupdate.com/202004/morocco-extends-facial-recognition-moratorium-to-year-end-proposes-biometric-authentication-service> [accessed 13 July 2022].

2.6 Related frameworks for assessing facial recognition

Given the current regulatory gap and the ongoing use of FRT, it is critical to assess how police are using the technology, which we aim to achieve through this audit. Here, we discuss how our sociotechnical audit relates to the following frameworks that can be used to assess algorithmic systems: regulatory audits, technical audits, impact assessments, and guidance. We summarise these frameworks in **Table 2**.

Framework	Description	How is it used?	When is it used?	Example(s)
Regulatory audit	Evaluates an algorithmic system against standards such as ethics or legality	Externally	After deployment	Sociotechnical audit of police use of facial recognition (this work)
Technical audit	Evaluates the technical aspects of an algorithmic system	Externally	After deployment	'Gender Shades' study of bias in commercial facial recognition
Impact assessment	Assesses the impacts of an algorithmic system in order to address its risks	Internally	Before deployment	Data protection impact assessment and equality impact assessment
Guidance	Provides advice or standards on the use of an algorithmic system	Internally	Before deployment	Information Commissioner's opinion on the use of live facial recognition

Table 2: Summary of frameworks for assessing algorithmic systems.

A **regulatory audit** evaluates the functioning of an algorithmic system with respect to standards such as ethics, legality, or quality assurance.[53] It is often used by external entities after deployment. Examples include the AI auditing framework developed by the Information Commissioner's Office and the University of Essex's report on the Metropolitan Police Service's live FRT trial and its compliance with human rights law.[54] However, to the best of our knowledge, there is no set of ethical and legal questions developed to externally evaluate any police FRT deployment in England and Wales, and our sociotechnical audit attempts to fill this gap.

[53] Ada Lovelace Institute, AI Now Institute, and Open Government Partnership, *Algorithmic Accountability for the Public Sector* (2021) <https://www.opengovpartnership.org/wp-content/uploads/2021/08/algorithmic-accountability-public-sector.pdf> [accessed 13 July]; Ada Lovelace Institute and DataKind UK, 'Examining the Black Box'.

[54] Information Commissioner's Office, *Guidance on the AI Auditing Framework: Draft Guidance for Consultation* (14 February 2020) <https://ico.org.uk/media/2617219/guidance-on-the-ai-auditing-framework-draft-for-consultation.pdf> [accessed 13 July]; Fussey and Murray, *Independent Report*.

A **technical audit** evaluates the functioning of an algorithmic system with respect to its technical elements such as reliability or algorithmic bias.[55] Similar to regulatory audits, technical audits are often used by external entities after deployment. Examples include the 'Gender shades' study of bias in commercial FRT and the 'Garbage In, Garbage Out' study of police use of FRT.[56] Such audits can be powerful tools in fostering greater algorithmic fairness and accountability.[57] While these audits focus on the technical performance of FRT, our sociotechnical audit incorporates broader legal and ethical considerations that these audits do not focus on.

An **impact assessment** assesses the impacts of an algorithmic system in order to address risks posed by the system, usually before implementation.[58] Impact assessments are often intended for internal use by the entities deploying the algorithmic system. Examples include the data protection impact assessment, the equality impact assessment, the conformity assessment in the proposed EU AI Act, the Ada Lovelace Institute's algorithmic impact assessment, and the ALGO-CARE framework for policing algorithms.[59]

In contrast to impact assessments that are often generic and focused on legal standards, our audit is context-specific and also considers ethical standards beyond the scope of the law. Further, our audit complements impact assessments: while impact assessments are tools for internal use before a deployment, our audit is a tool for external stakeholders after a deployment.

[55] Ada Lovelace Institute, AI Now Institute, and Open Government Partnership, *Algorithmic Accountability*; Ada Lovelace Institute and DataKind UK, 'Examining the Black Box'; Digital Regulation Cooperation Forum, *Auditing Algorithms: The Existing Landscape, Role of Regulators and Future Outlook* (28 April 2022) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1071554/DRCF_Algorithmic_audit.pdf> [accessed 13 July 2022].

[56] Buolamwini and Gebru, 'Gender Shades'; Clare Garvie, 'Garbage In, Garbage Out: Face Recognition on Flawed Data' (Georgetown: Centre on Privacy & Technology, 16 May 2019) <https://www.flawedfacedata.com/> [accessed 13 July].

[57] Inioluwa Deborah Raji and Joy Buolamwini, 'Actionable Auditing: Investigating the Impact of Publicly Naming Biased Performance Results of Commercial AI Products', *Conference on Artificial Intelligence, Ethics, and Society* (2019) <https://www.thetalkingmachines.com/sites/default/files/2019-02/aies-19_paper_223.pdf> [accessed 13 July 2022].

[58] Ada Lovelace Institute, AI Now Institute, and Open Government Partnership, *Algorithmic Accountability*; Ada Lovelace Institute and DataKind UK, 'Examining the Black Box'.

[59] 'Article 35 GDPR: Data Protection Impact Assessment', *General Data Protection Regulation (GDPR)*, Chapter 4 <https://gdpr.eu/article-35-impact-assessment/> [accessed 13 July 2022]; Doug Pyper, 'The Public Sector Equality Duty and Equality Impact Assessments', *House of Commons Library Briefing Paper*, 06591 (8 July 2020) <https://researchbriefings.files.parliament.uk/documents/SN06591/SN06591.pdf> [accessed 13 July]; European Commission, *Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) And Amending Certain Union Legislative Acts*, COM/2021/206 final (21 April 2021) <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206> [accessed 17 July 2022]; Ada Lovelace Institute, *Algorithmic Impact Assessment: A Case Study in Healthcare*, Ethics and Accountability in Practice (February 2022) <https://www.adalovelaceinstitute.org/project/algorithmic-impact-assessment-healthcare/> [accessed 13 July]; Marion Oswald and Sheena Unwin, 'Written Evidence Submitted to the House of Lords, Science and Technology Committee', *Algorithms in Decision-Making*, ALG0030 (23 May 2018) <http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/science-and-technology-committee/algorithms-in-decisionmaking/written/69002.html> [accessed 13 July 2022].

Context-specific regulatory guidance offers advice or standards provided by government or oversight bodies that are tailored to police use of FRT in England and Wales. Examples include the Information Commissioner's opinion on live FRT, the Surveillance Camera Code of Practice, the former Surveillance Camera Commissioner's guidance, and the College of Policing's Authorised Professional Practice on live FRT.[60]

In contrast to guidance developed for police, our audit provides a practical tool for external stakeholders to evaluate police use of FRT. Much context-specific guidance also comes from a legal perspective, and our audit builds on this by considering both legal and ethical standards.

General algorithmic guidance provides high-level advice or standards on the use of algorithmic systems. Examples include the UK Government's guide to using AI in the public sector, the UK Government's Data Ethics Framework, and the UK Algorithmic Transparency Standard.[61] While general algorithmic guidance tends to be broad and challenging to implement, our audit builds on such guidance and serves as a usable tool that reveals the particular risks of police use of FRT.

Compared to other frameworks, our sociotechnical audit is unique in two key aspects. First, in contrast to general assessments of algorithmic or AI systems, this audit is tailored to the context-specific risks of police use of facial recognition in England and Wales.

Second, the audit addresses both legal and ethical standards, whereas many other frameworks only focus on either one aspect or the other. We consider legal standards, as important values are reflected in the law such as the values of privacy and equality; aligning the audit with existing legal systems can also facilitate policy change. Additionally, we consider ethical standards, as there are important principles that go beyond the scope of the law such as community oversight; most importantly, just because we can do something does not mean that we should.

[60] Information Commissioner's Office, *Information Commissioner's Opinion: The Use of Live Facial Recognition Technology by Law Enforcement in Public Places*, ref. 2019/01 (31 October 2019) <https://ico.org.uk/media/about-the-ico/documents/2616184/live-frt-law-enforcement-opinion-20191031.pdf> [accessed 14 July 2022]; Home Office, *Surveillance Camera Code of Practice* (November 2021) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1035067/Surveillance_Camera_CoP_Accessible_PDF.pdf> [accessed 13 July 2022]; Anthony Porter, *Facing the Camera: Good Practice and Guidance for the Police Use of Overt Surveillance Camera Systems Incorporating Facial Recognition Technology to Locate Persons on a Watchlist, in Public Places in England & Wales* (November 2020) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/940386/6.7024_SCC_Facial_recognition_report_v3_WEB.pdf> [accessed 13 July 2022]; College of Policing, 'Live Facial Recognition', *Authorised Professional Practice* <https://www.college.police.uk/app/live-facial-recognition> [accessed 13 July 2022].

[61] Central Digital and Data Office and Office for Artificial Intelligence, 'A Guide to Using Artificial Intelligence in the Public Sector' (18 October 2019) <https://www.gov.uk/government/collections/a-guide-to-using-artificial-intelligence-in-the-public-sector> [accessed 13 July 2022]; Central Digital and Data Office, 'Data Ethics Framework' (16 September 2020) <https://www.gov.uk/government/publications/data-ethics-framework> [accessed 13 July]; Central Digital and Data Office, 'Algorithmic Transparency Standard' (7 July 2022) <https://www.gov.uk/government/collections/algorithmic-transparency-standard> [accessed 13 July 2022].

SECTION 3

MOTIVATION

3.1 Considerations before using this audit

We hope that this audit will become part of the larger conversation about whether police should use facial recognition technologies at all. However, given that police forces continue to adopt FRT, this audit can help outside stakeholders to expose deficiencies and scrutinise the use of the technology. The audit provides stakeholders with concrete questions to frame conversations about the ethics and legality of FRT deployments.

Experts in algorithmic auditing suggest that the purpose of an audit is to reveal blind spots rather than to green-light the use of a technology. An audit 'should not be considered as a reward to game or a goal to strive for, but a very low bar not to be caught tripping over'.[62] Thus, performing well on this audit does not green-light the adoption of FRT nor carry enough weight to overturn an existing moratorium. Rather, the audit can be used to evaluate whether the minimum ethical and legal standards to mitigate harm are met.

3.2 What is this audit for?

The audit can reveal the risks and harms of police use of FRT. The audit results can be used to expose deficiencies in the design and deployment of FRT and can be used as evidence when scrutinising police use of FRT. Example deficiencies include an inadequate legal basis, lack of community oversight, and discriminatory use of the technology on marginalised groups.

The audit can help evaluate compliance with the law and national guidance. The audit is contextualised for the England and Wales jurisdiction, with legal standards in the audit primarily informed by the Human Rights Act 1998, the Equality Act 2010, and the Data Protection Act 2018. National guidance from UK government bodies was also used to construct the audit. Note that performing well on the audit does not mean that a police force fully complies with the law. Rather, the audit is a starting point for legal risks that need to be considered.

The audit can inform policy, advocacy, and ethics scrutiny on police use of FRT. The audit can help scrutinise and improve transparency in how police are using FRT. The audit can be a starting point for greater accountability and can support policy and advocacy efforts on FRT. As researchers have noted, 'The outputs of audits, if made public, can make the system more legible to external actors (like regulators or the wider public), and therefore carries the potential to trigger other accountability mechanisms, including through public scrutiny or through regulatory action.'[63]

[62] Inioluwa Deborah Raji, Timnit Gebru, Margaret Mitchell, Joy Buolamwini, Joonseok Lee, and Emily Denton, 'Saving Face: Investigating the Ethical Concerns of Facial Recognition Auditing', *AAI/ACM Conference on Artificial Intelligence, Ethics, and Society* (2020), 145–51 <https://doi.org/10.1145/3375627.3375820>, p. 150.

[63] Ada Lovelace Institute, AI Now Institute, and Open Government Partnership, *Algorithmic Accountability for the Public Sector*, p. 25.

3.3 Who is this audit for?

In order for the audit to be meaningful, it should be administered by an external entity independent of the police. Auditor independence is crucial to mitigate conflicts of interest that would yield biased audit results.[64] Key stakeholders who we imagine might administer this audit or use the findings include:

- **Regulatory bodies** can use the audit to monitor and enforce the law for police use of FRT, administer inspections into how police are using FRT, and provide national guidance on FRT.
- **Oversight bodies** can use the audit to administer inspections into how police are using FRT, provide ethics scrutiny on police use of FRT, and improve public understanding on FRT.
- **Policymakers** can use the audit to inform debates, inquiries, and legislation on the use of FRT and other new technologies in law enforcement.
- **Civil society groups**, especially those working at the intersection of technology and human rights, can use the audit to campaign for policies such as an FRT ban, pursue strategic litigation that challenges police use of FRT, and provide expert evidence on FRT to government bodies.
- **The public**, especially impacted individuals or parties acting on their behalf, can use the audit to understand how police are using FRT and seek remedy for any resulting harm.

[64] Emanuel Moss, Elizabeth Anne Watkins, Ranjit Singh, Madeleine Clare Elish, and Jacob Metcalf, *Assembling Accountability: Algorithmic Impact Assessment for the Public Interest* (Data & Society, 29 June 2021) <http://dx.doi.org/10.2139/ssrn.3877437>, p. 24.

3.4 How to use this audit?

The audit can be conducted as an investigation after a police force's facial recognition deployment(s). For example, the audit can help to evaluate a police force's trial deployments of a particular type of FRT. The audit can also be used to assess a proposed or ongoing use of FRT, but the results may be limited based on what information is available.

Any evaluation using this audit should be based on information that is known and accessible to the public. This helps to assess how transparent police forces are with the public. Additionally, publishing key audit results can enable external scrutiny and mobilise change in whether and how FRT is implemented by police forces.[65] However, the degree of disclosure should be considered carefully, as publishing the audit results could enable people to green-light the adoption of FRT or misuse the results.[66]

[65] Moss and others, *Assembling Accountability*, p. 20.

[66] Sasha Costanza-Chock, Inioluwa Deborah Raji, and Joy Buolamwini, 'Who Audits the Auditors? Recommendations from a Field Scan of the Algorithmic Auditing Ecosystem', *ACM Conference on Fairness, Accountability, and Transparency* (2022), 1571–83 <https://doi.org/10.1145/3531146.3533213>, p. 1579.

SECTION 4

METHODOLOGY

To construct this audit, we translated high-level principles of ethics and legality into what they mean for practice within the specific context of police use of FRT in England and Wales. We define ethics by the principles of fairness, transparency, and accountability, and we define legality as compliance with the law in England and Wales. We describe these terms further in **Section 2.1**.

General AI ethics frameworks: We began with what ethics and legality mean in the general context of public sector use of data and AI systems. Here, we used frameworks developed by the UK government that reflect the types of questions and considerations the government expects public agencies including police forces to answer. Specifically, we used the UK Government's Data Ethics Framework, Guide to Using AI in the Public Sector, and Algorithmic Transparency Standard.[67] By consolidating and grouping questions from these sources, we arrived at an initial draft of the audit.

Literature review: We then adapted this initial draft to the specific context of police use of FRT in England and Wales using a review of existing literature. Most documents that we drew on were focused specifically on facial recognition, but we also used documents on surveillance, personal data, and new technologies more broadly. We revised the general audit questions and generated new questions based on documents from a variety of perspectives:

- **Users:** We examined documents on FRT developed by police forces in England and Wales to understand the current landscape and gaps in how police are using the technology.
- **Courts:** We drew upon legal challenges to police use of FRT and related court cases to gather perspectives from courts that interpret the laws.
- **Legislators:** We used reports developed by UK legislative committees on the use of FRT and other new technologies in the criminal justice system.
- **Regulators:** We incorporated guidance developed by UK regulatory bodies on FRT and compliance with data protection law.
- **Academia:** We drew upon academic evaluations of police use of FRT in England and Wales to understand known ethical and legal issues that have arisen in past FRT deployments.

[67] Central Digital and Data Office, 'Data Ethics Framework'; Central Digital and Data Office and Office for Artificial Intelligence, 'Understanding Artificial Intelligence Ethics and Safety' (10 June 2019) <https://www.gov.uk/guidance/understanding-artificial-intelligence-ethics-and-safety> [accessed 13 July]; Central Digital and Data Office, 'Algorithmic Transparency Standard'.

- **Advisors:** We leveraged resources on data and technology usage developed by oversight or advisory bodies such as local ethics committees, professional bodies, and government entities.
- **Auditors:** We examined evaluations conducted by algorithmic auditors to test the reliability and performance of FRT systems.
- **Civil society:** We used resources on FRT and AI governance developed by civil society groups focused on protecting privacy, human rights, and civil liberties in the digital age.

In **Section 5**, we discuss the sources used to develop each section of the audit. In **Appendix C**, we detail the specific sources used to generate each question of the audit.

Stakeholder feedback: Finally, we revised the audit based on informal feedback from stakeholders holding many of the perspectives listed above, including those within police organisations, government, academia, and civil society. We spoke with a total of 35 stakeholders to understand the current landscape of police use of FRT in the UK and to gather feedback on aspects that might be missing from the audit.

Based on feedback and discussions, we added and removed questions, and adapted the content and arrangement of questions. These conversations with stakeholders predominantly occurred virtually using video-conferencing tools, although a few took place in person or over email. Individuals who agreed to be acknowledged are included in the **Acknowledgements**.

Case studies: We applied the audit to three case studies: (1) *Bridges* case on South Wales Police's trial of live facial recognition, (2) Metropolitan Police Service's trial of live facial recognition, and (3) South Wales Police's trial of mobile phone facial recognition. We selected these case studies based on several factors: (a) notability of the cases, (b) a sample of different police forces, and (c) different types of facial recognition being used. We identified gaps and a lack of clarity in some questions when we applied the audit to these case studies, so we subsequently refined the audit.

SECTION 5

STRUCTURE OF THE SOCIOTECHNICAL AUDIT

The audit comprises the following four sections: (1) Legal Standards, (2) Technical Reliability, (3) Human Decision-Making, and (4) Expertise and Oversight. Each section includes a comprehensive set of questions grouped by subsections, summarised in **Table 3**. Questions in both the Legal Standards section and the Technical Reliability section are aligned with existing legislation. We present these questions thus to assess the performance of FRT and broader considerations related to how FRT is used.

Audit Section	Description	Subsections
Legal Standards	Evaluates how police demonstrate their legal compliance for the use of facial recognition	In Accordance with the Law Necessary in a Democratic Society Data Protection Non-Discrimination Free Expression and Assembly
Technical Reliability	Evaluates the reliability of facial recognition and the rigour and transparency of police evaluations	Algorithmic Fairness Robust Practice Deployment Performance
Human Decision-Making	Evaluates how facial recognition changes police decisions	Human Review Preparation Accountability
Expertise and Oversight	Evaluates the expertise and oversight over police use of facial recognition	Ethics Committee Civil Society and Experts Community Engagement

Table 3: Summary of the sections of the sociotechnical audit.

Audit scoring: The audit is composed of yes/no questions that are scored with either **1 (yes)** or **0 (no)** accompanied by an explanation.[68] We choose to use a scoring mechanism as it helps make the audit practical and simple to use. Specifically, scoring helps (a) produce consistent results when different auditors evaluate a given police force, (b) compare the evaluation results across different police forces, and (c) summarise the audit results and identify where there are deficiencies. In **Section 8**, we consider the limitations of this scoring mechanism.

Below, we discuss the subsections and limitations for each section of the audit. See **Appendix C** for further details about the sources used to generate each question of the audit and the provisions of law to which questions refer.

5.1 Legal standards

The Legal Standards section evaluates how police demonstrate their legal compliance for the use of facial recognition. FRT engages with several rights protected by the Human Rights Act 1998, including the right to privacy and the rights to freedom of expression and assembly.[69] To be lawful, any interference with these rights must be (a) in accordance with the law, (b) in pursuit of a legitimate aim, and (c) necessary in a democratic society.[70] FRT also interferes with rights established in the Equality Act 2010 and the Data Protection Act 2018.

To construct the Legal Standards section, we leveraged the *R (Bridges) v. Chief Constable of South Wales Police* court case that found deficiencies in South Wales Police's compliance with human rights, equality, and data protection law. We reviewed additional case law, police policy documents, and academic evaluations of police use of FRT. Additionally, we drew on guidance from the UK Information Commissioner, European Data Protection Supervisor, and European Court of Human Rights.

[68] This audit scoring was inspired by the non-profit WhiteCoats4BlackLives' Racial Justice Report Card (RJRC), which is an initiative that evaluates the extent to which academic medical centres in the United States promote racial justice. We use a similar design to the RJRC for our Sociotechnical Audit Scorecard.

[69] The *Bridges* case held that Article 8 privacy rights of the Human Rights Act 1998 are engaged 'if biometric data is captured, stored and processed, even momentarily' which holds for any facial recognition technology.

[70] Steven Greer, *The Exceptions to Articles 8 and 11 of the European Convention on Human Rights*, Human Rights Files, 15 (Strasbourg: Council of Europe, 1997) <https://www.echr.coe.int/LibraryDocs/DG2/HRFILES/DG2-EN-HRFILES-15(1997).pdf> [accessed 13 July 2022]; *Big Brother Watch and Others v. the United Kingdom, Judgement*, ECtHR 439, app. nos 58170/13, 62322/14, and 24960/15 (25 May 2021) <http://www.bailii.org/eu/cases/ECHR/2021/439.html> [accessed 13 July 2022], para. 332; This audit focuses on the 'in accordance with the law' and the 'necessary in a democratic society' requirements, as policing activities typically satisfy the legitimate aim of public safety or the prevention of disorder or crime. For example, see *Catt v. the United Kingdom, Judgement*, ECtHR 76, app. no. 43514/15 (24 January 2019) <http://www.bailii.org/eu/cases/ECHR/2019/76.html> [accessed 13 July 2022], para. 108.

The Legal Standards section of the audit comprises questions grouped by the following subsections.

1. In Accordance with the Law (Human Rights Act 1998)
Evaluates whether there are clear, objective, and limited criteria with regard to the watchlist construction, usage of FRT, and access to the data. Under the Human Rights Act 1998, any interference with Article 8 privacy rights must meet the 'in accordance with the law' requirement.[71] In the *Bridges* case, the Court of Appeal found that this requirement was not satisfied, as the criteria for who was included in the watchlist and where FRT was used were not clear and objective and left too broad of a discretion to police officers. In this subsection, we consider these factors but note that they are not exhaustive to satisfy the 'in accordance with the law' requirement.

2. Necessary in a Democratic Society (Human Rights Act 1998)
Evaluates whether police demonstrate that their use of FRT meets the legal test of 'necessary in a democratic society' established in the Human Right Act 1998.[72] Under the Human Rights Act 1998, an interference with Article 8 privacy rights must satisfy the 'necessary in a democratic society' test. This legal test is not a test of FRT's usefulness, but involves addressing FRT's interference with human rights in a democratic society. Necessity and proportionality are both part of the 'necessary in a democratic society' test based on the case law of the European Court of Human Rights.

3. Data Protection (Data Protection Act 2018)
Evaluates whether police demonstrate their compliance with the data protection requirements mandated by the Data Protection Act 2018, the General Data Protection Regulation, and standards established by the Information Commissioner. This includes publishing an adequate impact assessment that complies with data protection principles, and enabling individuals to exercise their data protection rights.[73] This subsection refers to Part 3 of the Data Protection Act 2018 and Chapters 2 to 4 of the General Data Protection Regulation.

4. Non-Discrimination (Human Rights Act 1998 and Equality Act 2010)
Evaluates whether police demonstrate their compliance with equality standards based on Article 14 of the Human Rights Act 1998 and the Public Sector Equality Duty of the Equality Act 2010. This includes publishing an equality impact assessment and publishing demographic data on the use of FRT to understand the risk of certain demographic groups being disproportionately targeted.[74]

[71] To be 'in accordance with the law', the legal basis must be published and understandable ('accessible') and should not leave too broad of a discretion to police officers ('foreseeable') in order to protect against arbitrary interference. Some questions in this subsection on the 'in accordance with the law' requirement also tie into the 'necessary in a democratic society' test. The 'in accordance with the law' test is linked to the 'necessary in a democratic society' test in that the legal framework should limit permissible activity to that which is necessary in a democratic society.

[72] The Data Protection Act 2018 mandates a separate strict necessity test for the processing of personal data, but this audit focuses on the 'necessary in a democratic society' test established in the Human Rights Act 1998.

[73] The first question in the Data Protection subsection assesses *whether* police have carried out and published a data protection impact assessment (DPIA) and an appropriate policy document (APD) for sensitive data processing, as mandated by the Data Protection Act 2018. The remaining questions in the Data Protection subsection aim to assess the *quality* of the DPIA and APD.

[74] The first question in the Non-Discrimination subsection assesses *whether* police have carried out and published an equality impact assessment (EIA). The remaining questions in the Non-Discrimination subsection and questions in the Technical Reliability section aim to assess the *quality* of the EIA.

5. Free Expression and Assembly (Human Rights Act 1998)
Evaluates the extent to which police consider the rights to freedom of expression and assembly, which are protected under Articles 10 and 11 of the Human Rights Act 1998. The use of FRT can generate a 'chilling effect' on these rights, where individuals refrain from expressing ideas and engaging in democratic processes such as protests. Assessing the impact on these rights is essential in the analysis of whether the use of FRT satisfies the 'necessary in a democratic society' legal requirement.

There are several limitations to what the audit can assess for legal standards, which we outline below.

Lack of an adequate legal framework for FRT: As we discuss in **Section 2.5**, the current legal framework governing the use of FRT is insufficient. Currently, there is no explicit legal basis and primary legislation for police use of FRT. The 'in accordance with the law' requirement established in the Human Rights Act 1998 requires that the measure in question (a) has some basis in domestic law and (b) be compatible with the rule of law.[75]

These aspects have been disputed in the context of police use of FRT. For (a), police forces often rely on broad common law policing duties as a legal basis, but this has been criticised for being overly ambiguous and insufficient.[76] For (b), the Court of Appeal in the *Bridges* case pointed out the lack of clear guidance for who is included in the watchlist and where FRT is deployed. Other factors could include whether additional data or analytics are used with FRT, and how FRT might be used in the future. Many argue that the 'in accordance with the law' requirement cannot be satisfied when there is no dedicated legislation for the use of new technologies such as FRT.[77]

[75] *Catt v. the United Kingdom*, para. 94.

[76] Woods, 'United Kingdom – Automated Facial Recognition in the UK'; Fussey and Murray, *Independent Report*; Privacy International and others, 'Consultation on Live Facial Recognition APP'.

[77] Pete Fussey, Daragh Murray, and Amy Stevens, 'Written Evidence Submitted to the Justice and Home Affairs Committee', *New Technologies and the Applications of the Law*, NTL0017 (21 October 2021) <https://committees.parliament.uk/writtenevidence/38635/html/> [accessed 13 July 2022]. There is debate about whether the common law, coupled with a police force's publicly available policy documents, can satisfy the 'in accordance with the law' requirement. Many argue that this is not possible. The Court of Appeal in the *Bridges* case left this open; the Court noted that this could be sufficient 'in principle'.

Ordering for legal tests: Legal tests should be evaluated in a particular order. For example, if a measure does not pass the 'in accordance with the law' requirement, there is no need to examine its necessity, as this first part of legality is not met. Similarly, if a measure does not satisfy the necessity test, there is no need to examine its proportionality, as necessity is a precondition for proportionality.[78] Although we encourage the audit questions to be completed in order, this audit enables the assessment of legal tests even if their precondition is not met.

Legislation is not a silver bullet: While legal issues from the use of FRT are important to consider, there are also relevant ethical concerns that are not covered by legislation. It is critical that ethical issues are considered given that there is currently a lack of primary legislation governing police use of FRT (see **Section 2.5**). While this section of the audit focuses on legal standards, other sections assess the use of FRT against ethical standards, such as independent oversight, that may not be required by the current legal framework.

Limited use of case law: Due to time constraints, we were not able to conduct an in-depth review of the case law on surveillance from the European Court of Human Rights. The case law could be used to add more detail around the relevant legal safeguards and to strengthen the legal standards set by this audit.

5.2 Technical reliability

The Technical Reliability section evaluates the reliability of facial recognition and the rigour and transparency of police evaluations. Here, we assess the extent to which police mitigate algorithmic bias and ensure FRT's reliability in a transparent manner, primarily based on standards established by the *Bridges* case and regulatory guidance from the UK Information Commissioner.

Facial recognition has been found to perform worse on women, people of colour, and people with disabilities, and police forces are required by the Public Sector Equality Duty of the Equality Act 2010 to understand this bias in FRT.[79] Additionally, police forces often consider FRT to be a tool that helps prevent crime, bring offenders to justice, and prevent threats to public security.[80] However, poor performance of FRT raises human rights concerns for those misidentified and challenges the effectiveness of the technology in achieving these stated goals.[81]

[78] European Data Protection Supervisor, *Guidelines on Assessing the Proportionality of Measures that Limit the Fundamental Rights to Privacy and to the Protection of Personal Data* (19 December 2019) <https://edps.europa.eu/sites/default/files/publication/19-12-19_edps_proportionality_guidelines2_en.pdf> [accessed 13 July 2022].

[79] Buolamwini and Gebru, 'Gender Shades'; Byrne-Haber, 'Disability and AI Bias'.

[80] Metropolitan Police Service, 'Live Facial Recognition'.

[81] Privacy International and others, 'Consultation on Live Facial Recognition APP', p. 8.

The Technical Reliability section of the audit comprises questions grouped by the following subsections.

1. Algorithmic Fairness (Equality Act 2010)
Evaluates whether police transparently evaluate bias inherent in FRT. The Public Sector Equality Duty of the Equality Act 2010 requires that police take reasonable steps to assess whether the FRT software has bias, based on the *Bridges* court case. We consider whether police carry out and publish an evaluation of bias to assess if there is demonstrated compliance with the Public Sector Equality Duty.

2. Robust Practice (Data Protection Act 2018)
Evaluates whether there are measures to ensure and assess FRT's accuracy. If FRT is inaccurate and yields too many incorrect matches, this challenges the fairness and necessity of the personal data processing, which are mandated by Part 3 the Data Protection Act 2018.

3. Deployment Performance (Equality Act 2010)
Evaluates whether police demonstrate that FRT performs well and similarly across demographic groups, as mandated by the Public Sector Equality Duty of the Equality Act 2010 and based on performance metrics recommended by the Information Commissioner.[82]

There are several limitations to what the audit can assess for technical reliability, which we outline below.

Technical improvements do not green-light FRT: Improving FRT's performance does not remove the risks posed by the technology. As advocates have articulated, 'While adding more diverse training data or taking other measures to improve accuracy may address some current issues with these systems, this will ultimately only perfect them as instruments of surveillance and make them more effective at undermining our rights.'[83] Thus, we might not want to improve FRT's performance in the first place, as doing so could render certain groups hypervisible and more likely to be recognised, exposing them to systems of surveillance.[84]

Exclusion of marginalised communities: Evaluations of algorithmic bias often rely on rigid and binary classifications such as men/women to measure differences in FRT performance across groups. However, these evaluations may not capture how bias impacts people differently, especially those who fall outside or between classifications. For example, evaluations that use binary gender classifications can exclude non-binary, transgender, and gender non-conforming people, exacerbating harms against these already vulnerable communities.[85]

[82] Information Commissioner's Office, *Information Commissioner's Opinion: The Use of Live Facial Recognition Technology in Public Places* (18 June 2021) <https://ico.org.uk/media/2619985/ico-opinion-the-use-of-lfr-in-public-places-20210618.pdf> [accessed 13 July 2022], p. 65.

[83] Access Now and others, 'Open Letter Calling for a Global Ban on Biometric Recognition Technologies', p. 3.

[84] Benjamin, *Race after Technology*, Chapter 3.

[85] Raji and others, 'Saving Face', p. 147.

Unethically trained facial recognition: In the effort to reduce algorithmic bias, FRT developers have sought to construct large and diverse datasets, sometimes, via unethical practices that often disproportionately impact marginalised communities.[86] For example, Google targeted Black people who were homeless to improve the performance of its software across demographic groups.[87] Although this audit does not capture these harms, they are critical to consider if police forces are to use facial recognition.

5.3 Human decision-making

The Human Decision-Making section assesses how facial recognition changes police decisions. The use of FRT by police has high stakes, as the output of the technology can substantially impact individuals and communities, for example, through a wrongful arrest. These consequences can be exacerbated depending on how police use the technology and what accountability measures are in place for impacted persons. For example, because technology is often seen as objective, police may defer to the decision made by the FRT system, raising the concern that the technology becomes the decision-maker.

In this section, we assess these complex human-technology interactions, primarily based on considerations highlighted by the UK Justice and Home Affairs Committee, academic evaluations of police use of FRT, and civil society perspectives on the EU AI Act.

The Human Decision-Making section of the audit comprises questions grouped by the following subsections.

1. Human Review
Evaluates whether there is a 'human in the loop' by assessing if police officers provide a reliable review of FRT matches. This is critical to evaluate since FRT-generated matches may be incorrectly viewed as objective and can 'prime' officers to view those matched as suspicious.[88]

2. Preparation
Evaluates whether there are measures including police training and a non-operational trial to ensure that police are prepared to use the technology.

3. Accountability
Evaluates whether there is accountability and remedy for harms resulting from the use of FRT in policing, and whether there is protection for whistleblowers who may expose these harms in the first place.

[86] Raji and others, 'Saving Face'.

[87] Jack Nicas, 'Atlanta Asks Google Whether It Targeted Black Homeless People', *New York Times* (4 October 2019) <https://www.nytimes.com/2019/10/04/technology/google-facial-recognition-atlanta-homeless.html> [accessed 13 July 2022].

[88] Pete Fussey, Bethan Davies, and Martin Innes, '"Assisted" Facial Recognition and the Reinvention of Suspicion and Discretion in Digital Policing', *British Journal of Criminology*, 61.2 (2020), 325–44 <https://doi.org/10.1093/bjc/azaa068>; Pete Fussey and Daragh Murray, 'Policing Uses of Live Facial Recognition in the United Kingdom', in *Regulating Biometrics: Global Approaches and Urgent Questions*, ed. by Amba Kak (New York: AI Now Institute, 2020), pp. 78–85 <https://ainowinstitute.org/regulatingbiometrics-fussey-murray.pdf> [accessed 13 July 2022]; Fussey and others, 'Written Evidence Submitted to the Justice and Home Affairs Committee'.

There are limitations to what the audit can assess for human decision-making, which we outline below.

Wider changes in policing: This audit does not encapsulate all of the wider changes that occur when police use FRT regardless of the safeguards in place. FRT adoption can shift police behaviour and suspicion, and the public space where FRT is used can become an area of over-policing.[89] For example, at FRT deployments, stop and searches and racial profiling unrelated to the technology have arisen.[90] Police officers have also been found to ask individuals for proof of immigration status during facial recognition deployments. These changes point to how the technology can exacerbate the harms against people of colour and immigrant populations.

5.4 Expertise and oversight

The Expertise and Oversight section evaluates the expertise and oversight over police use of facial recognition. External scrutiny throughout the lifecycle of police use of FRT is critical for accountability. Oversight is necessary not only prior to deployments but also regularly during deployments, for example, to assess the legitimacy, necessity, and proportionality of each deployment.

The UK Justice and Home Affairs Committee report on technologies in the justice system recommends that: 'Local specialist ethics committees are best placed to scrutinise technological solutions throughout their lifecycle and in their deployment contexts.'[91] In addition to ethics committees, the wider public also plays an important role in proper oversight. Affected communities are experts on the impacts of surveillance technologies; thus, centring the voices of marginalised communities in decisions about FRT is essential.[92]

In this section, we assess the extent to which there is meaningful oversight, based on resources developed by the Justice and Home Affairs Committee and the Biometrics and Forensics Ethics Group, as well as academia, civil society, and existing ethics committees in the UK.

[89] Fussey and others, '"Assisted" Facial Recognition'; Big Brother Watch, *Briefing on Facial Recognition Surveillance* (June 2020) <https://bigbrotherwatch.org.uk/wp-content/uploads/2020/06/Big-Brother-Watch-briefing-on-Facial-recognition-surveillance-June-2020.pdf> [accessed 13 July 2022].

[90] Big Brother Watch, *Briefing on Facial Recognition Surveillance*.

[91] House of Lords, Justice and Home Affairs Committee, *Technology Rules?*, p. 75.

[92] 'Jennifer Lee on Privacy, Surveillance and Civil Rights', *The Good Robot* (University of Cambridge Centre for Gender Studies, 7 September 2021) <https://www.buzzsprout.com/1786427/9146359-jennifer-lee-on-privacy-surveillance-and-civil-rights> [accessed 13 July 2022]; American Civil Liberties Union, 'Tech Equity Coalition' <https://www.aclu-wa.org/pages/tech-equity-coalition> [accessed 13 July 2022].

The Expertise and Oversight section of the audit comprises questions grouped by the following subsections.

1. Ethics Committee
Evaluates whether there is continuing oversight from an ethics committee throughout the FRT project, and whether this oversight is diverse, effective, and sustainable.

2. Civil Society and Experts
Evaluates whether there are proactive and effective consultations with civil society and independent experts on the use of facial recognition.

3. Community Engagement
Evaluates whether there is community oversight on the use of FRT from the wider public, especially marginalised communities, and whether information about police use of FRT is accessible.

There are limitations to what the audit can assess for expertise and oversight, which we outline below.

Ethics committees are just one approach to oversight: We evaluate the extent to which there is meaningful oversight from an ethics committee. Although ethics committees may be well placed to provide oversight, they are just one mechanism and independent oversight can come from other places.

Challenge of meaningful oversight: For oversight to be meaningful, it must be independent and hold the power to influence police use of FRT. However, there may be a trade-off between the independence of an oversight body and its ability to influence police. Current structures in policing might make it challenging to have both. For example, an ethics committee situated within a Police and Crime Commissioner's office may have the ability to influence the police force, but might have a conflict of interest with the force.

SECTION 6

SOCIOTECHNICAL AUDIT SCORECARD

We present this sociotechnical audit as a tool for external stakeholders to assess the ethics and legality of police use of FRT. Contextualised for England and Wales, the audit should be used to reveal risks and harms, not green-light the adoption of FRT. The audit questions are not exhaustive and not to be treated as a checklist. We note that currently there is no explicit legal basis for police use of FRT.

See **Section 2.2** for a primer on FRT and **Appendix C** for definitions of terms used in the audit questions below.

Audit scoring: Each yes/no question of the audit is scored with either **1 (yes)** or **0 (no)** accompanied by an explanation. If the answer is unknown or inaccessible to the public, the question is scored with **0 (no)**. Note that there is no partial credit when scoring each question. Each subsection is then scored by the number of questions within it that scored **1 (yes)**.

6.1 Legal standards

In Accordance with the Law (Human Rights Act 1998)

A. Are there clear, objective, and limited criteria for who can be included in the watchlist, including with regard to the image source and the seriousness of offence or risk?

B. Are there clear, objective, and limited criteria for where and when FRT can be used, including mandating reasonable suspicion that persons on the watchlist will be at the location and requiring a high grade of intelligence for the police intelligence case that supports FRT use?

C. Are there clear, objective, and limited criteria concerning third-party access to the data collected or retained, including with regard to what data can be shared, with whom it can be shared, and for what specific purpose it can be shared?

Score: / 3

Necessary in a Democratic Society (Human Rights Act 1998)

D. Have police identified less intrusive alternative measures and proven that FRT is strictly necessary compared to these measures using scientifically verifiable evidence?

E. Have police conducted distinct necessity tests with an evidence-based justification for each category of individuals on the watchlist?

F. Have police shown that FRT does not disproportionately limit the human rights of affected persons, including those who are misidentified, not on the watchlist, or impacted by unwarranted intrusions?

Score: / 3

Data Protection (Data Protection Act 2018)

G. Before using FRT, have police carried out and published a data protection impact assessment and appropriate policy document for sensitive data processing?

H. Beyond social media or website publishing, have police used other means to inform potential data subjects or most people in their jurisdiction in advance about when, where, why, and how FRT is being used and how they can exercise their individual rights?

I. Are there clear measures to ensure data subjects can exercise their individual rights including the rights to rectification, erasure, and object with clear justifications if exemptions apply?

J. Do police check the watchlist against the data source close to the time of deployment to ensure the watchlist is accurate and up to date?

K. Are there clear measures to ensure that watchlist images are lawfully held, have a known provenance, and exclude unconvicted custody images?

L. Via direct consultation, have police proactively considered views of the public, especially marginalised communities, on the particular type of FRT and justified a disregard of the views if relevant?

M. Have police published their procurement contracts and data-sharing agreements with other parties?

Score: / 7

Non-Discrimination (Human Rights Act 1998 and Equality Act 2010)

N. Before using FRT, have police carried out and published an equality impact assessment?

O. For each deployment, have police published the demographic makeup of the watchlist?

P. For each deployment, have police published the demographic makeup of the population where FRT is used?

Q. For each deployment, have police published the demographic data for arrests, stop and searches, and other outcomes resulting from the use of FRT?

Score: / 4

Free Expression and Assembly (Human Rights Act 1998)

R. Have police assessed FRT's potential 'chilling effect' on the rights to freedom of expression and assembly to inform the legal test of 'necessary in a democratic society'?

S. Do police preclude using FRT to identify those peacefully participating in an assembly?

Score: / 2

6.2 Technical Reliability

Algorithmic Fairness (Equality Act 2010)

A. Before using FRT, have police evaluated and published the demographic makeup of the training dataset to ensure the dataset is representative of the population where it is to be used?

B. Before using FRT, have police evaluated and published FRT's performance across demographic groups, in different conditions that match FRT's operational use, to ensure FRT performs well and similarly across the population?

Score: / 2

Robust Practice (Data Protection Act 2018)

C. Are there safeguards precluding the use of FRT with an unsuitable low-quality probe or watchlist image?

D. Have police pre-established and met thresholds for the FRT system's accuracy (precision, false positive rate, true positive rate) to inform the legal test of strict necessity for personal data processing?

Score: / 2

Deployment Performance (Equality Act 2010)

E. Does FRT perform well (precision, false positive rate, true positive rate) and similarly across demographic groups?

Score: / 1

6.3 Human decision-making

Human Review

A. Is there a transparent evaluation that shows human review of the FRT matches is reliable, given the accuracy of officer-verified matches and the amount of time an officer has to review an FRT match?

Score: / 1

Preparation

B. Is training for the particular type of FRT mandated for police officers using the technology?

C. Are there clear standards for technical training on using FRT, data protection training, and training on risks including differential treatment, function creep, and unwarranted intrusions?

D. Has there been a documented non-operational research trial of FRT with informed consent from participants before the operational use of FRT for policing?

Score: / 3

Accountability

E. Are there clear measures for police to document cases of harm resulting from the use of FRT such as differential treatment, function creep, or unwarranted intrusions?

F. Do police have a whistleblower protection policy to protect persons who reveal FRT misuse?

G. Is there a clear redress mechanism (beyond judicial review and usual complaint procedures) for harmed individuals and groups to participate in an investigation into police use of FRT?

H. Are there clear measures to ensure that the redress mechanism is procedurally fair?

Score: / 4

6.4 Expertise and oversight

Ethics Committee

A. Is regular oversight from an ethics committee mandated throughout the life of the FRT project?

B. Are there clear processes for the committee to influence if and how FRT is implemented, including the power of veto for the FRT project?

C. Is the committee an independent body from police organisations with members having non-policing backgrounds and with safeguards to ensure the committee's sustainability even without political support?

D. Is the committee diverse in terms of demographic makeup and independent expertise in human rights, equality, and data protection?

E. Are detailed meeting minutes published, including briefing papers, discussions, and conclusions?

Score: / 5

Civil Society and Experts

F. Are there transparent, proactive consultations with civil society and independent experts on the particular type of FRT?

G. Are police required to consider the advice from consultations and transparently explain the outcomes, including providing a justification if the advice is not followed?

Score: / 2

Community Engagement

H. Are there clear, proactive processes for the public, especially marginalised communities, to influence if and how FRT is implemented?

I. Are all FRT materials accessible to people with disabilities and provided in immigrant languages?

Score: / 2

SECTION 7

SOCIOTECHNICAL AUDIT CASE STUDIES

We applied this sociotechnical audit to three cases to show how the audit can be used in practice and to evaluate real-world facial recognition deployments in England and Wales.

7.1 *Bridges* case on South Wales Police's trial of live facial recognition

Our first case study is of the operational trial deployments of live facial recognition (LFR) conducted by South Wales Police (SWP) from May 2017 to April 2019.[93] In *R (Bridges) v. Chief Constable of South Wales Police*, the Court of Appeal ruled that these deployments were unlawful as 'there was no clear guidance on where [LFR] could be used and who could be put on a watchlist, a data protection impact assessment was deficient and the force did not take reasonable steps to find out if the software had a racial or gender bias'.[94] We highlight additional legal and ethical concerns beyond the scope of the court case, including the technology's use at protests and the absence of effective oversight.

[93] At the time of the deployments, South Wales Police called the technology live automated facial recognition (AFR) or AFR Locate.

[94] Jenny Rees, 'Facial Recognition Use by South Wales Police Ruled Unlawful', *BBC Wales* <https://www.bbc.co.uk/news/uk-wales-53734716> [accessed 13 July 2022].

SWP did not establish limits on the use of LFR at assemblies. In fact, the technology was used at a peaceful anti-arms protest, interfering with the human rights to freedom of expression and assembly, without evidence that the legal requirements of necessity and proportionality were met.[95] SWP's data protection impact assessment and policy documents did not acknowledge nor address LFR's impact on the rights to freedom of expression and assembly.

There was a lack of effective oversight over the use of LFR. While SWP had early engagements with the SWP Joint Independent Ethics Committee, regular and transparent oversight was not provided throughout the lifecycle of the LFR project.[96] During committee meetings, there were no independent experts in human rights, equality, or data protection in attendance, even though such expertise has been documented as crucial for the oversight of technologies such as LFR.

Moreover, there remained concerns about the committee's independence. Although there were some independent members, the committee also included police officers and is a body situated within the police force. In fact, during meetings, 63% of attendees were members of SWP and 71% were members of either SWP or the South Wales Police and Crime Commissioner. Finally, there were no consultations with the public, especially marginalised communities, on how and whether LFR was implemented.

Below is a summary of the audit scorecard for this case study. See **Appendix D** for the full case study, which includes an explanation for each audit question.

[95] A Emily Apple, 'South Wales Police Under Fire for Using Facial Recognition Technology Against Protesters', *The Canary* (29 March 2018) <https://www.thecanary.co/uk/2018/03/29/south-wales-police-under-fire-for-using-facial-recognition-technology-against-protesters/> [accessed 13 July]; Big Brother Watch, *Face Off: The Lawless Growth of Facial Recognition in UK Policing* (May 2018) <https://bigbrotherwatch.org.uk/wp-content/uploads/2018/05/Face-Off-final-digital-1.pdf> [accessed 13 July].

[96] The committee's published meeting minutes indicate that there was only one meeting where LFR was discussed, yet this discussion itself is not published.

Case Study #1:

Bridges case on South Wales Police's trial of live facial recognition

Police Force: South Wales Police (SWP)

Facial Recognition Type: Live Facial Recognition (LFR)

LFR Deployment Dates: Trial deployments from May 2017 to April 2019

Audit Evaluation Date: July 2022

Key Resources Used: ***Bridges* Case**, **SWP Documents**, **Deployment Results**, **Cardiff University Report**[97]

Full Case Study Link: **Appendix D**

Subsections with a score of zero are highlighted in light red.

METRIC	SCORE AND NOTES	
1. Legal Standards (Human Rights Act 1998, Equality Act 2010, Data Protection Act 2018)		
In accordance with the law	0 / 3	Lack of clear limits for watchlist, usage, and data access
Necessary in a democratic society	0 / 3	Inadequate necessity and proportionality assessments
Data protection	2 / 7	Up to date watchlist, but inadequate measures to ensure rights
Non-discrimination	1 / 4	No published demographic data for watchlist, usage, and arrests
Free expression and assembly	0 / 2	No assessment of chilling effect; no limit on LFR at protests

[97] South Wales Police, *Smarter Recognition, Safer Community* <https://afr.south-wales.police.uk/smarter-recognition/> [accessed 13 July 2022]; *R (Bridges) v. Chief Constable of South Wales Police*, Judgement, Court of Appeal; South Wales Police, 'List of Previous FRT Deployments'; Bethan Davies, Martin Innes, and Andrew Dawson, *An Evaluation of South Wales Police's Use of Automated Facial Recognition* (Cardiff: Universities' Police Science Institute, 2018) <https://afr.south-wales.police.uk/wp-content/uploads/2019/10/AFR-EVALUATION-REPORT-FINAL-SEPTEMBER-2018.pdf> [accessed 13 July 2022].

METRIC	SCORE AND NOTES	
2. Technical Reliability (Equality Act 2010, Data Protection Act 2018)		
Algorithmic fairness	0 / 2	No evaluation of LFR's data bias or algorithmic bias
Robust practice	0 / 2	Low-quality images could be used; no pre-established thresholds
Deployment performance	0 / 1	Poor LFR precision of 24%; different accuracy across gender
3. Human Decision-Making		
Human review	0 / 1	Human review of LFR-generated matches had 69% precision
Preparation	0 / 3	Only technical training; lack of training for initial deployments
Accountability	0 / 4	Whistleblower policy only created in 2019; lack of redress for harms
4. Expertise and Oversight		
Ethics committee	0 / 5	Lack of regular oversight; lack of diversity and independence
Civil society and experts	0 / 2	Lack of proactive and effective consultations on LFR use
Community engagement	0 / 2	Lack of community oversight; lack of accessible documents

7.2 Metropolitan Police Service's trial of live facial recognition

The next case study is of the operational trial deployments of live facial recognition (LFR) conducted by the Metropolitan Police Service (MPS) from August 2016 to February 2019. We build upon a study conducted by University of Essex researchers on the human rights compliance of these trials. Their report concludes that the trials would likely 'be held unlawful if challenged before the courts' given the absence of clear guidance on who was included in a watchlist and the failure to establish that LFR was 'necessary in a democratic society' as required by human rights law.[98] We found additional concerns related to discrimination and oversight.

While MPS published some demographic data in their results, they did not record the demographic breakdown for engagements, stop and searches, arrests, and other outcomes resulting from the use of LFR. This makes it hard to evaluate whether LFR perpetuates racial profiling. There was also no published evaluation of racial or gender bias in the technology. MPS conducted an internal evaluation but did not disclose the results. This lack of transparency makes it difficult for outside stakeholders to assess the comprehensiveness of the evaluation.

[98] Fussey and Murray, *Independent Report*. p. 6.

Since the trial deployments have ended, MPS has frequently pointed to an evaluation undertaken by the National Institute of Standards & Technology.[99] However, citing this evaluation can be misleading: even though the evaluation shows a high accuracy, it was conducted with high-quality standardised images rather than low-quality wild images on which LFR was used.[100] The absence of a published evaluation in conditions that match LFR's use is especially concerning given that the same technology used by MPS misidentified and led to wrongful arrests of Black men in the United States.[101]

With regard to oversight, MPS engaged with the London Policing Ethics Panel (LPEP). However, transparent oversight began after several deployments rather than starting from the concept stage of the trial. Even though MPS responded to the panel's recommendations, the panel was advisory and MPS was not required to act upon the recommendations. There were also no experts in human rights, equality, or data protection on the panel, even though this has been documented as crucial for the oversight of LFR.

The summary of the audit scorecard is below and see **Appendix E** for the full case study.

[99] Nicholas Ephgrave, 'MPS Response to the London Policing Ethics Panel Final Report on Live Facial Recognition Technology' (23 January 2020) <http://www.policingethicspanel.london/uploads/4/4/0/7/44076193/met_response_to_lpep_live_facial_recognition_report.pdf> [accessed 13 July 2022]; Metropolitan Police Service, 'Equality Impact Assessment' <https://www.met.police.uk/SysSiteAssets/media/downloads/force-content/met/advice/lfr/impact-assessments/lfr-eia.pdf> [accessed 13 July 2022]; Patrick Grother, Mei Ngan, and Kayee Hanaoka, 'Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects', National Institute of Standards and Technology Interagency or Internal Report, 8280 (December 2019) <https://doi.org/10.6028/NIST.IR.8280>.

[100] Currently, MPS is testing the performance of LFR with the National Physical Laboratory during operational deployments. This evaluation is expected to complete in the third quarter of 2022, significantly after numerous deployments have already occurred. The data collected during the evaluation may also be shared with the UK law enforcement community and its partners, raising concerns about broad access and potential function creep.

[101] MPS procured its LFR technology from the company NEC Corporation. NEC's facial recognition technology was used by police in the United States in 'cases of Black men wrongfully accused of crimes they did not commit in Detroit and New Jersey, as the underlying algorithm for facial recognition provided by contractor DataWorks Plus', 'NEC Corp', *Investigate: A Project of the American Friends Service Committee* (25 October 2021) <https://investigate.afsc.org/company/nec> [accessed 13 July 2022]. See also: Kashmir Hill, 'Wrongfully Accused by an Algorithm', *New York Times* (24 June 2020) <https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html> [accessed 13 July 2022]; Martin Coulter, 'A Black Man Spent 10 Days in Jail After He Was Misidentified by Facial Recognition, a New Lawsuit Says', *Business Insider* (29 December 2020) <https://www.businessinsider.com/black-man-facial-recognition-technology-crime-2020-12?r=MX&IR=T> [accessed 13 July 2022].

Case Study #2:

Metropolitan Police Service's trial of live facial recognition

Police Force: Metropolitan Police Service (MPS)

Facial Recognition Type: Live Facial Recognition (LFR)

LFR Deployment Dates: Trial deployments from August 2016 to February 2019

Audit Evaluation Date: July 2022

Key Resources Used: **MPS DPIA**, **MPS Legal Mandate**, **MPS Report**, **Essex University Report**[102]

Full Case Study Link: **Appendix E**

Subsections with a score of zero are highlighted in light red.

METRIC	SCORE AND NOTES	
1. Legal Standards (Human Rights Act 1998, Equality Act 2010, Data Protection Act 2018)		
In accordance with the law	1 / 3	Limits for data access, but lack of limits for watchlist and usage
Necessary in a democratic society	0 / 3	Inadequate necessity and proportionality assessments
Data protection	0 / 7	Issues of inaccurate data; inadequate measures to ensure rights
Non-discrimination	0 / 4	Some demographics provided, but not for arrests and outcomes
Free expression and assembly	0 / 2	No assessment of chilling effect; no limit on LFR at protests

[102] Nigel Nelson, 'Metropolitan Police Service Privacy Impact Assessment' (25 July 2019) <https://www.statewatch.org/media/documents/news/2018/dec/uk-metropolitan-police-service-privacy-impact-assessment-lfr.pdf> [accessed 13 July 2022]; Bernie Galopin and Nigel Nelson, 'Live Facial Recognition, (LFR) MPS Legal Mandate' (23 July 2019) <https://www.statewatch.org/media/documents/news/2018/dec/uk-live-facial-recognition-lfr-mps-legal-mandate.pdf> [accessed 13 July 2022]; National Physical Laboratory and Metropolitan Police Service, *Metropolitan Police Service Live Facial Recognition Trials*; Fussey and Murray, *Independent Report*.

METRIC	SCORE AND NOTES	
2. Technical Reliability (Equality Act 2010, Data Protection Act 2018)		
Algorithmic fairness	0 / 2	No published evaluation of LFR's data bias or algorithmic bias
Robust practice	0 / 2	Low-quality images could be used; no pre-established thresholds
Deployment performance	0 / 1	Poor LFR precision of 19%; different accuracy across gender
3. Human Decision-Making		
Human review	0 / 1	Human review of LFR-generated matches had 36% precision
Preparation	0 / 3	No mandated training for LFR; lack of non-operational trial
Accountability	0 / 4	Lack of whistleblower protection; lack of redress for harms
4. Expertise and Oversight		
Ethics committee	0 / 5	Lack of oversight from the start; lack of diversity and veto power
Civil society and experts	0 / 2	Lack of proactive and effective consultations on LFR use
Community engagement	0 / 2	Lack of community oversight; lack of accessible documents

7.3 South Wales Police's trial of mobile phone facial recognition

Our final case study is of the recent operational trial of mobile phone or operator initiated facial recognition (OIFR) conducted by South Wales Police (SWP) from December 2021 to March 2022.[103] SWP provided more documentation about their use of OIFR in comparison with their trial of live facial recognition, which was ruled unlawful in the *Bridges* court case. Although there were improvements, significant gaps remain with regard to the minimum legal and ethical standards. We highlight the lack of (a) limited criteria for who is included in the watchlist, (b) full transparency for evaluations of discrimination, and (c) independent oversight and community engagement.

First, the watchlist included all custody images of South Wales Police with no limits on the seriousness of offence.[104] This broad inclusion raises concerns about the legal requirements of necessity and proportionality, especially whether distinct necessity tests for each category of individuals on the watchlist were conducted. Moreover, the watchlist included the images of innocent persons who were arrested but not convicted, even though these images are unlawful to retain.[105]

[103] In December 2021, Gwent Police reported that they would be trialling OIFR alongside South Wales Police using the same policies. However, in April 2022, Gwent Police responded to a freedom of information request stating that, 'We can confirm that the Operator Initiated Facial Recognition app is not used within Gwent Police due to technical issues': Gwent Police, 'Response to Freedom of Information Request 2022/25016 – Facial Recognition Technology' <https://www.gwent.police.uk/foi-ai/gwent-police/disclosure2/2022/04---april/202225016---facial-recognition-technology/> [accessed 13 July 2022]. There is no transparency about the details of these technical issues.

[104] Custody images are photographs taken by police when an individual is arrested.

[105] South Wales Police considers the deletion of unconvicted custody images upon request and is actively working to find a solution to automatically remove these images. However, currently unconvicted custody images are still included in the watchlist by default, even though they are unlawful to retain. See *RMC and FJ v. Commissioner of Police for the Metropolis and Secretary of State for the Home Department, Judgement*, High Court, Queen's Bench Division, cases CO/12476/2010 and CO/5572/2011 (22 June 2012) <https://www.judiciary.uk/wp-content/uploads/JCO/Documents/Judgments/r-rmc-fj-metropolitan-police-commissioner-22062012.pdf> [accessed 13 July 2022].

Second, while SWP took proactive steps to evaluate bias and discrimination, there was a lack of full transparency for these evaluations. SWP evaluated OIFR's accuracy before its operational use and found no evidence of algorithmic bias. However, SWP did not publish the demographic distribution of the evaluation dataset, which is crucial to assess bias. Additionally, SWP provided the demographic data for the people on which OIFR was used, but the demographic data for the watchlist and those arrested remain unknown.

Finally, there were notable gaps in oversight and community engagement. SWP engaged with the SWP Joint Independent Ethics Committee before and after the OIFR trial. However, the committee consists of police officers and is a body situated within the police, raising concerns about the independence of the oversight. Based on the most recently published meeting minutes, there were no independent experts in human rights, equality, or data protection on the committee. Moreover, SWP did not conduct consultations with the public, nor with civil society, to gather feedback before or during the OIFR trial.

The summary of the audit scorecard is below and see **Appendix F** for the full case study.

Case Study #3:

South Wales Police's trial of mobile phone facial recognition

Police Force: South Wales Police (SWP)

Facial Recognition Type: Mobile Phone or Operator Initiated Facial Recognition (OIFR)

OIFR Deployment Dates: Trial deployments from December 2021 to March 2022

Audit Evaluation Date: July 2022

Key Resources Used: **SWP Documents**, **SWP EIA**, **SWP Deployment Results**[106]

Full Case Study Link: **Appendix F**

Subsections with a score of zero are highlighted in light red.

METRIC	SCORE AND NOTES	
1. Legal Standards (Human Rights Act 1998, Equality Act 2010, Data Protection Act 2018)		
In accordance with the law	0 / 3	Lack of limits for data access and the offence type for watchlist
Necessary in a democratic society	0 / 3	Inadequate necessity and proportionality assessments
Data protection	1 / 7	Up to date watchlist, but inadequate measures to ensure rights
Non-discrimination	1 / 4	Some demographics provided, but not for watchlist and arrests
Free expression and assembly	0 / 2	No assessment of chilling effect; no limit on OIFR at protests

[106] South Wales Police, 'Operator Initiated Facial Recognition Documents' <https://www.south-wales.police.uk/police-forces/south-wales-police/areas/about-us/about-us/facial-recognition-technology/operator-initiated-facial-recognition-documents/> [accessed 13 July 2022]; South Wales Police, 'Equality Impact Assessment: Facial Recognition Technology – Retrospective, Live and Operator Initiated' (10 August 2021) <https://drive.google.com/file/d/1yuH0e4tsFKDofTz-diloltbVHpOBH3t-/view?usp=sharing> [accessed 13 July 2022]; South Wales Police, 'Facial Recognition App Pilot Results' (29 April 2022) <https://www.south-wales.police.uk/news/south-wales/news/2022/ebr-apr/pilot-results-for-the-new-facial-recognition-app/> [accessed 13 July 2022].

METRIC	SCORE AND NOTES	
2. Technical Reliability (Equality Act 2010, Data Protection Act 2018)		
Algorithmic fairness	0 / 2	Unknown demographics of training and evaluation datasets
Robust practice	0 / 2	Low-quality images could be used; no pre-established thresholds
Deployment performance	1 / 1	OIFR match returned as the top result on every occasion of use
3. Human Decision-Making		
Human review	0 / 1	No published evaluation of the human review of OIFR matches
Preparation	2 / 3	Non-operational trial conducted, but unclear training standards
Accountability	1 / 4	Whistleblower protection, but lack of redress for harms
4. Expertise and Oversight		
Ethics committee	1 / 5	Some oversight provided, but lack of diversity and independence
Civil society and experts	0 / 2	Lack of proactive and effective consultations on OIFR use
Community engagement	0 / 2	Lack of community oversight; lack of accessible documents

SECTION 8

LIMITATIONS OF THE SOCIOTECHNICAL AUDIT

1. This audit does not capture all harms related to police use of FRT.

Performing well on this audit does not green-light the use of FRT, as the audit does not fully capture the known and potential risks of the technology. We discuss the limitations of each individual section of the audit in **Section 5** of this report.

The audit may also not capture the harms that happen in practice or behind closed doors. There may be a significant discrepancy between how police intend or claim to use FRT and how police implement FRT in practice. The audit results may depend on how transparent police are with the public and how much access an auditor has to the use of FRT. For instance, while an individual can observe a live FRT deployment, the use of retrospective FRT does not provide the same opportunity, making its harms less transparent.

Additionally, there are wider harms in public-private partnerships that the audit does not capture. For example, many UK police forces use surveillance cameras developed by Hikvision, a business linked with the persecution of Uyghurs in China, which raises serious concerns about the role of police forces in supporting companies involved in broader human rights abuses.[107]

2. Using this audit to improve transparency alone cannot create accountability.

This audit can help make police use of FRT more visible, yet this visibility is not sufficient to govern the use of the technology. For example, the audit can reveal an inadequate human rights assessment or the lack of community engagement. However, exposing such deficiencies in police use of FRT is not equivalent to holding police accountable, although it can be a starting point for accountability.[108] For example, if unlawful or unethical police practices continue after they have been made transparent, then we must focus on changing the power imbalance between the police and the public that this ineffectiveness reveals.[109]

[107] House of Commons, Foreign Affairs Committee, *Never Again*; Sampson, 'Letter from the Biometrics and Surveillance Camera Commissioner'; Big Brother Watch, *Who's Watching You*?

[108] Mike Ananny and Kate Crawford, 'Seeing Without Knowing: Limitations of the Transparency Ideal and Its Application to Algorithmic Accountability', *New Media & Society*, 20.3 (2018), 973–89 <https://doi.org/10.1177/1461444816676645>, p. 985.

[109] Ananny and Crawford, 'Seeing Without Knowing', p. 984.

3. Auditor independence is critical for this audit to provide meaningful scrutiny.

There is a risk that the audit does not provide meaningful scrutiny if the auditor is not independent. For example, a police force auditing their own use of FRT would be similar to them marking their own homework.[110]

However, even if the auditor is formally independent, they might have a conflict of interest with the police.[111] This could soften the evaluation and turn the audit into a box-ticking exercise. For instance, police councils, police ethics committees, and private companies hired by police may not be effective auditors because of their conflict of interest and their potential motivations to produce results in favour of the police.

Refer to **Section 10** for the positionality of the author of this work.

4. This audit's yes/no questions make the audit simple but may miss complexities in an evaluation.

The audit contains yes/no questions that are accompanied by explanations evidencing how each answer was obtained. These yes/no questions help make the audit simple to use and produce more consistent results. However, such binary questions may not capture the complexity of many situations in an evaluation.

5. This audit does not have a perfect scoring mechanism to assess police use of FRT.

We provide a simple scoring mechanism to help summarise the audit results on how a given police force is using FRT. Future work may entail developing an enhanced mechanism that (a) gives partial credit for audit questions that have been partly satisfied and (b) provides weights to questions in order to prioritise critical ones.

6. This audit may be limited by the lack of information about police use of retrospective FRT.

The audit was primarily informed by materials on live FRT and mobile phone FRT. Currently, there is little information on how police forces in England and Wales are using retrospective facial recognition in practice. The audit questions still extend to retrospective FRT, but they might be limited due to the lack of information about this particular type of facial recognition.

[110] Marion Oswald, 'A Three-Pillar Approach to Achieving Trustworthy and Accountable Use of AI and Emerging Technology in Policing in England and Wales: Lessons from the West Midlands Data Ethics Model', *European Journal of Law and Technology*, 13.1 (2022) <https://ejlt.org/index.php/ejlt/article/view/883/1045> [accessed 14 July 2022], p. 2.

[111] Moss and others, *Assembling Accountability*, p. 24.

SECTION 9

CONCLUSION

Globally and in the UK, police forces continue to adopt and deploy facial recognition technology. We have presented a sociotechnical audit to evaluate this ongoing use of facial recognition. Our audit will hopefully become part of larger conversations around the implications and limitations of police use of FRT. We hope that this work will lead to questions about whether police should use facial recognition technologies at all.

Given the proliferation of FRT deployments, our audit establishes a set of minimum ethical and legal standards for the governance of the technology. We have found that these minimum standards are not met by police forces in the three case studies that we present here. We have shown how police use of facial recognition fails to incorporate many of the known practices for the safe and ethical use of large-scale data systems. This problem moves well beyond the concern of bias in facial recognition algorithms.

It has been demonstrated that police use of FRT is very broad in scope and may infringe upon human rights such as the right to privacy. By evaluating the documents that police forces make public, we have highlighted that some deployments may not be 'in accordance with the law' or 'necessary in a democratic society', as required by human rights law.

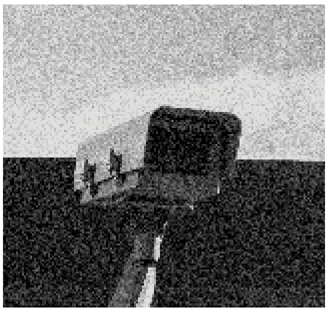
Our results also show a lack of proactive consultations with the public, especially marginalised communities that might be most affected by FRT deployments. Additionally, police force documents are not fully accessible to people with disabilities or provided in immigrant languages. This lack of accessibility makes it difficult for certain groups to understand how FRT impacts them and to seek remedy in the case of harm.

We have also found that much information about police use of facial recognition is kept from public view. This lack of transparency limits the external scrutiny of police use of FRT. For example, there is little published demographic data on the arrests and outcomes resulting from the use of FRT. This makes it difficult to evaluate whether or not these tools perpetuate racial profiling.

Transparency, however, does not equate to accountability. Police forces are not necessarily answerable or held responsible for FRT harms. For all three case studies and more broadly, there is no clear framework to ensure accountability for the misuse or failure of FRT.[112] There is a lack of robust redress mechanisms for individuals and communities harmed by police deployments of the technology.

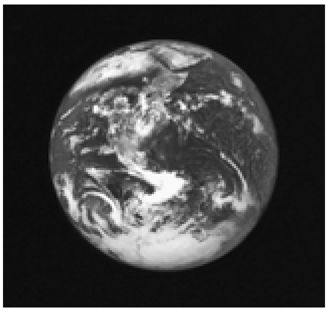
[112] House of Lords, Justice and Home Affairs Committee, *Technology Rules?*, p. 37.

Based on these research findings, we present the following recommendations, encouraging policymakers, regulators, civil society groups, and researchers to:



1. Use this audit to scrutinise police use of facial recognition.

The audit can be leveraged to understand the extent to which facial recognition deployments meet the minimum ethical and legal standards. We encourage others to engage with the broad range of questions about ethics and legality that this audit brings together. The audit can be used to gather evidence and inform strategic litigation efforts to challenge police use of facial recognition.



2. Evaluate the use of biometric technologies in other contexts and regions.

Future work may refine this audit for other biometric tools such as gait analysis and emotion recognition, or even other technologies, such as predictive models and automatic number plate recognition, based on the risks that they pose. The audit could also be adapted to assess the risks that such technologies pose in different environments. We call for a greater focus on how technologies are used in specific geographical and historical contexts, including outside the UK and in the Global South.

3. Join calls for a ban on police use of facial recognition in public spaces.

This audit shows that some facial recognition deployments fail to meet minimum ethical and legal standards. We highlight the lack of (a) evidence of a lawful interference with privacy rights, (b) transparent evaluations of discrimination, (c) measures for remedy for harmed persons, and (d) regular oversight from an independent ethics body and the wider community.

Moreover, the current legal framework for governing facial recognition is not fit for purpose.[113] The existing legal framework is insufficient to protect against the harms of FRT use by police forces. Given this existing regulatory gap and the failure to meet minimum standards, we support calls for a ban on police use of facial recognition in publicly accessible spaces.

[113] Ryder, *The Ryder Review*, p. 11.

While this report focuses on the adoption of facial recognition by police, this work relates to the use of surveillance technologies more broadly, including by private entities. The line between the public and private sector is becoming increasingly blurred, as police and private companies often collaborate in the development and deployment of facial recognition.[114]There has also been an increasing use of surveillance technologies in schools and shops, where there are similar concerns of privacy, discrimination, accountability, and oversight.[115]

To protect human rights and improve accountability in how technology is used, we must ask what values we want to embed in technology and also move from high-level values and principles into practice. Furthermore, we need greater consideration not just about technologies, but about the broader structures in our society.

We hope this work is a step in this direction.

[114] Biometrics and Forensics Ethics Group, *Briefing Note*, p. 5.

[115] Sally Weale, 'ICO to Step in After Schools Use Facial Recognition to Speed Up Lunch Queue', *The Guardian* (18 October 2021) <https://www.theguardian.com/education/2021/oct/18/privacy-fears-as-schools-use-facial-recognition-to-speed-up-lunch-queue-ayrshire-technology-payments-uk> [accessed 14 July 2022]; Matt Burgess, 'Co-op is Using Facial Recognition Tech to Scan and Track Shoppers', *Wired* (18 December 2020) <https://www.wired.co.uk/article/coop-facial-recognition> [accessed 14 July 2022].

SECTION 10

POSITIONALITY STATEMENT

The author of this work is motivated to understand and expose harm in how technological systems are used in our society. They are committed to challenge technologies that infringe upon human rights and perpetuate the oppression of marginalised communities. This view has shaped this audit.

The author does not have any affiliation with a police service organisation. The author's research work is funded by the Rotary Foundation Global Grant Scholarship. The author is a Visiting Fellow at the Minderoo Centre for Technology and Democracy, an academic research centre at the University of Cambridge focused on rethinking the power relationships between digital technologies, society, and our planet.

The author welcomes ideas and critical feedback on any sections of this report.

SECTION 11

ABOUT THE AUTHOR

Evani Radiya-Dixit is a Visiting Fellow at the Minderoo Centre for Technology and Democracy at the University of Cambridge and a 2021–22 Rotary Scholar. She is interested in questions of technology, accountability, and power.

Evani completed her bachelor's degree in Computer Science from Stanford University and will be pursuing her master's degree in Sociology at Stanford. Previously, she worked on machine learning projects at Nvidia and Google. Her research has been published at the International Conference on Learning Representations, the Stanford Public Interest Technology Lab, and the think tank New America.

Recently, she presented at the ACM Conference on Fairness, Accountability, and Transparency. With her interest in public service, Evani has worked at the U.S. federal Cybersecurity and Infrastructure Security Agency and contributed to a data privacy strategy for a city council in California.

SECTION 12

ACKNOWLEDGEMENTS

I would like to express sincere thanks to those who informed the work behind this audit through feedback and discussions. These include: Andrew Strait (Ada Lovelace Institute), Ann Kristin Glenster (University of Cambridge), Areeq Chowdhury (Royal Society), Ben Bradford (University College London), Daragh Murray (University of Essex), Emmanuelle Andrews (Liberty), Fraser Sampson (Biometrics and Surveillance Camera Commissioner), Griff Ferris (Fair Trials), Ioannis Kouvakas (Privacy International), Jenny Brennan (Ada Lovelace Institute), Jun Pang (Liberty), Jyoti Belur (University College London), Katrina Ffrench (Unjust), Katy Watts (Liberty), Lorna Woods (University of Essex), Madeleine Chang (Ada Lovelace Institute), Mher Hakobyan (European Disability Forum), Nour Haidar (Privacy International), Nóra Ní Loideáin (University of London), Paul Quinton (College of Policing), Pete Fussey (University of Essex), and Tom McNeil (West Midlands Police and Crime Commissioner's Office). These individuals had differing views on whether police should use facial recognition. They provided input on their own behalf, not on behalf of their affiliated organisation.

I am immensely grateful to my wonderful supervisor Professor Gina Neff for guiding me through the many pivots and learnings throughout this project. I am indebted to her for providing invaluable feedback, mentorship, and encouragement. I would like to extend my thanks to Jeremy Hughes, Irene Galandra Cooper, and the entire team at the Minderoo Centre for their generous support.

This work would not have been possible without the support and funding from the Rotary Foundation. I would like to thank the Cambridge Sawston, Grass Valley, and Nevada City Rotary Club members, especially Bill Boon for being a remarkable champion throughout my journey.

I would like to express huge thanks to my peers and friends – especially Bhumika Billa, Divij Joshi, and Julia Słupska – who shared comments on this report and supported me.

Last but not least, I am grateful to my community and family for their tremendous support during my time in the UK.

BIBLIOGRAPHY

Access Now, Amnesty International, European Digital Rights, Human Rights Watch, Internet Freedom Foundation, Instituto Brasileiro de Defesa do Consumidor, and others, 'Open Letter Calling for a Global Ban on Biometric Recognition Technologies that Enable Mass and Discriminatory Surveillance' (21 December 2021) <https://www.accessnow.org/ban-biometric-surveillance/> [accessed 12 July 2022]

Ada Lovelace Institute, *Algorithmic Impact Assessment: A Case Study in Healthcare*, Ethics and Accountability in Practice (February 2022) <https://www.adalovelaceinstitute.org/project/algorithmic-impact-assessment-healthcare/> [accessed 13 July]

Ada Lovelace Institute, AI Now Institute, and Open Government Partnership, *Algorithmic Accountability for the Public Sector* (2021) <https://www.opengovpartnership.org/wp-content/uploads/2021/08/algorithmic-accountability-public-sector.pdf> [accessed 13 July]

Ada Lovelace Institute and DataKind UK, 'Examining the Black Box: Tools for Assessing Algorithmic Systems, Identifying Common Language for Algorithm Audits and Impact Assessments' (29 April 2020) <https://www.adalovelaceinstitute.org/report/examining-the-black-box-tools-for-assessing-algorithmic-systems/> [accessed 12 July 2022]

American Civil Liberties Union, 'Tech Equity Coalition' <https://www.aclu-wa.org/pages/tech-equity-coalition> [accessed 13 July 2022]

———, 'Community Control Over Police Surveillance (CCOPS) Model Bill' (April 2021) <https://www.aclu.org/legal-document/community-control-over-police-surveillance-ccops-model-bill?redirect=other/community-control-over-police-surveillance-ccops-model-bill> [accessed 14 July 2022]

Amnesty International, *Trapped in the Matrix: Secrecy, Stigma, and Bias in the Mat's Gangs Database* (May 2018) <https://www.amnesty.org.uk/files/reports/Trapped%20in%20the%20Matrix%20Amnesty%20report.pdf> [accessed 12 July 2022]

———, 'UK: Dark Day for Civil Liberties as "Deeply-Authoritarian" Policing Bill Passed by Lords' (27 April 2022) <https://www.amnesty.org.uk/press-releases/uk-dark-day-civil-liberties-deeply-authoritarian-policing-bill-passed-lords> [accessed 12 July]

Ananny, Mike, and Kate Crawford, 'Seeing Without Knowing: Limitations of the Transparency Ideal and Its Application to Algorithmic Accountability', *New Media & Society*, 20.3 (2018), 973–89 <https://doi.org/10.1177/1461444816676645>

Apple, Emily, 'South Wales Police Under Fire for Using Facial Recognition Technology Against Protesters', *The Canary* (29 March 2018) <https://www.thecanary.co/uk/2018/03/29/south-wales-police-under-fire-for-using-facial-recognition-technology-against-protesters/> [accessed 13 July]

'Article 35 GDPR: Data Protection Impact Assessment', *General Data Protection Regulation (GDPR)*, Chapter 4 <https://gdpr.eu/article-35-impact-assessment/> [accessed 13 July 2022]

Automated Facial Recognition Technology (Moratorium and Review), HL Bill 87, 2019–21 (London: HMSO, 2020) <https://bills.parliament.uk/bills/2610> [accessed 13 July 2022]

BBC News, 'Download Festival: Leicestershire Police Defend Facial Recognition Scans' (15 June 2015) <https://www.bbc.co.uk/news/uk-england-leicestershire-33132199> [accessed 14 July 2022]

———, 'Black Police Leader Says Some Forces "Still Institutionally Racist"' (17 January 2018) <https://www.bbc.co.uk/news/uk-england-42702432> [accessed 12 July 2022]

———, 'South Wales Police to Use Facial Recognition App on Phones' (7 August 2019) <https://www.bbc.co.uk/news/uk-wales-49261763> [accessed 14 July 2022]

Benjamin, Ruha, *Race After Technology: Abolitionist Tools for the New Jim Code* (Cambridge: Polity, 2019)

Big Brother Watch, *Stop Facial Recognition* <https://bigbrotherwatch.org.uk/campaigns/stop-facial-recognition/> [accessed 13 July 2022]

———, *Face Off: The Lawless Growth of Facial Recognition in UK Policing* (May 2018) <https://bigbrotherwatch.org.uk/wp-content/uploads/2018/05/Face-Off-final-digital-1.pdf> [accessed 13 July]

———, Joint Statement on Police and Private Company Use of Facial Recognition Surveillance in the UK' (September 2019) <https://bigbrotherwatch.org.uk/wp-content/uploads/2019/09/Statement-to-stop-live-facial-recognition-surveillance-BBW-September-2019-1.pdf> [accessed 13 July 2022]

———, *Briefing on Facial Recognition Surveillance* (June 2020) <https://bigbrotherwatch.org.uk/wp-content/uploads/2020/06/Big-Brother-Watch-briefing-on-Facial-recognition-surveillance-June-2020.pdf> [accessed 13 July 2022]

———, 'Written Evidence for the Justice and Home Affairs Committee's Inquiry into New Technologies and the Application of the Law' (September 2021) <https://bigbrotherwatch.org.uk/wp-content/uploads/2022/05/Final-Big-Brother-Watch-Briefing-to-JHAC-on-new-technologies-and-the-application-of-the-law-Final10476.pdf> [accessed 14 July 2022]

———, *Who's Watching You? The Dominance of Chinese-State Owned CCTV in the UK* (7 February 2022) <https://bigbrotherwatch.org.uk/wp-content/uploads/2022/02/Whos-Watching-You_The-dominance-of-Chinese-state-owned-CCTV-in-the-UK.pdf> [accessed 12 July 2022]

Big Brother Watch and Open Rights Group, 'Joint Submission to the Scottish Parliament Justice Sub-Committee on Policing Inquiry into Facial Recognition: How Policing in Scotland Makes Use of this Technology' (November 2019) <https://bigbrotherwatch.org.uk/wp-content/uploads/2019/11/Big-Brother-Watch-and-Open-Rights-Group-Joint-Submission-to-the-Scottish-Justice-Sub-Committee-on-Policing-inquiry-into-Facial-Recognition-November-2019.pdf> [accessed 14 July 2022]

Big Brother Watch and Others v. the United Kingdom, Judgement, ECtHR 439, app. nos 58170/13, 62322/14, and 24960/15 (25 May 2021) <http://www.bailii.org/eu/cases/ECHR/2021/439.html> [accessed 13 July 2022]

Biometrics and Forensics Ethics Group, *Briefing Note on the Ethical Issues Arising from Public-Private Collaboration in the Use of Live Facial Recognition Technology* (January 2021) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/953359/LFR_briefing_note_18.1.21.final.pdf> [accessed 12 July 2022]

Bischoff, Paul, 'Facial Recognition Technology (FRT): 100 Countries Analyzed' (8 June 2021) <https://www.comparitech.com/blog/vpn-privacy/facial-recognition-statistics/> [accessed 13 July 2022]

Browne, Simone, *Dark Matters: On the Surveillance of Blackness* (Durham: Duke University Press, 2015)

Buolamwini, Joy, and Timnit Gebru, 'Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification', *Proceedings of Machine Learning Research*, 81 (2018), 1–15 <https://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf> [accessed 12 July 2022]

Buolamwini, Joy, Vincente Ordóñez, Jamie Morgenstern, and Erik Learned-Miller, *Facial Recognition Technologies: A Primer* (29 May 2020) <https://assets.website-files.com/5e027ca188c99e3515b404b7/5ed1002058516c11edc66a14_FRTsPrimerMay2020.pdf> [accessed 12 July 2022]

Burgess, Matt, 'Co-op is Using Facial Recognition Tech to Scan and Track Shoppers', *Wired* (18 December 2020) <https://www.wired.co.uk/article/coop-facial-recognition> [accessed 14 July 2022]

Burt, Chris, 'Morocco Extends Facial Recognition Moratorium to Year-End, Proposes Biometric Authentication Service' (9 April 2020) <https://www.biometricupdate.com/202004/morocco-extends-facial-recognition-moratorium-to-year-end-proposes-biometric-authentication-service> [accessed 13 July 2022]

Byrne-Haber, Sheri, 'Disability and AI Bias', *Medium* (11 July 2019) <https://sheribyrnehaber.medium.com/disability-and-ai-bias-cced271bd533> [accessed 12 July 2022]

Cabinet Office, 'Consultation Principles: Guidance', *Gov.uk* (19 March 2018) <https://www.gov.uk/government/publications/consultation-principles-guidance> [accessed 14 July 2022]

Catt v. the United Kingdom, Judgement, ECtHR 76, app. no. 43514/15 (24 January 2019) <http://www.bailii.org/eu/cases/ECHR/2019/76.html> [accessed 13 July 2022]

Central Digital and Data Office, 'Data Ethics Framework' (16 September 2020) <https://www.gov.uk/government/publications/data-ethics-framework> [accessed 13 July]

———, 'Algorithmic Transparency Standard' (7 July 2022) <https://www.gov.uk/government/collections/algorithmic-transparency-standard> [accessed 13 July 2022]

Central Digital and Data Office and Office for Artificial Intelligence, 'Understanding Artificial

Intelligence Ethics and Safety' (10 June 2019) <https://www.gov.uk/guidance/understanding-artificial-intelligence-ethics-and-safety> [accessed 13 July]

———, 'A Guide to Using Artificial Intelligence in the Public Sector' (18 October 2019) <https://www.gov.uk/government/collections/a-guide-to-using-artificial-intelligence-in-the-public-sector> [accessed 13 July 2022]

Cheshire Constabulary, 'Retrospective Facial Recognition Technology (RFR): Stage 2 – Data Protection Impact Assessment' (15 October 2021) <https://www.cheshire.police.uk/SysSiteAssets/media/downloads/cheshire/about-us/facial-recognition-technology/data-protection-impact-assessment-dpia-retrospective-frt.docx> [accessed 14 July 2022]

———, 'Operator Initiated Facial Recognition (OIFR) Legal Mandate' (10 June 2022) <https://www.cheshire.police.uk/SysSiteAssets/media/downloads/cheshire/about-us/facial-recognition-technology/oifr-legal-mandate.docx> [accessed 14 July 2022]

Chowdhury, Areeq, *Unmasking Facial Recognition: An Exploration of the Racial Bias Implications of Facial Recognition Surveillance in the United Kingdom* (London: WebRoots Democracy, 2020) <https://webrootsdemocracy.files.wordpress.com/2020/08/unmasking-facial-recognition-webroots-democracy.pdf> [accessed 14 July 2022]

College of Policing, 'Live Facial Recognition', *Authorised Professional Practice* <https://www.college.police.uk/app/live-facial-recognition> [accessed 13 July 2022]

———, 'Intelligence Report', *Authorised Professional Practice* <https://www.college.police.uk/app/intelligence-management/intelligence-report> [accessed 14 July 2022]

———, 'Terminology', *Authorised Professional Practice* (22 March 2022) <https://www.college.police.uk/print/pdf/node/3005> [accessed 12 July 2022]

———, 'Watchlist', *Authorised Professional Practice* (22 March 2022) <https://www.college.police.uk/print/pdf/node/3002> [accessed 12 July 2022]

Costanza-Chock, Sasha, Inioluwa Deborah Raji, and Joy Buolamwini, 'Who Audits the Auditors? Recommendations from a Field Scan of the Algorithmic Auditing Ecosystem', *ACM Conference on Fairness, Accountability, and Transparency* (2022), 1571–83 <https://doi.org/10.1145/3531146.3533213>

Coulter, Martin, 'A Black Man Spent 10 Days in Jail After He Was Misidentified by Facial Recognition, a New Lawsuit Says', *Business Insider* (29 December 2020) <https://www.businessinsider.com/black-man-facial-recognition-technology-crime-2020-12?r=MX&IR=T> [accessed 13 July 2022]

Cradle Community, *Brick by Brick: How We Build a World Without Prisons* (London: Hajar, 2021)

Cromarty, Hannah, 'Gypsies and Travellers', *House of Commons Library Briefing Paper*, 08083 (9 May 2019) <https://researchbriefings.files.parliament.uk/documents/CBP-8083/CBP-8083.pdf> [accessed 14 July 2022]

Cumber, Robert, 'Watchdog Responds to Facial Recognition Trial at Meadowhall in Sheffield', *The Star* (30 January 2020) <https://www.thestar.co.uk/news/crime/watchdog-responds-facial-recognition-trial-meadowhall-sheffield-1379265> [accessed 14 July 2022]

Dave, Paresh, 'U.S. Cities Are Backing Off Banning Facial Recognition as Crime Rises' (12 May 2022) <https://www.reuters.com/world/us/us-cities-are-backing-off-banning-facial-recognition-crime-rises-2022-05-12/> [accessed 13 July]

Davies, Bethan, Martin Innes, and Andrew Dawson, *An Evaluation of South Wales Police's Use of Automated Facial Recognition* (Cardiff: Universities' Police Science Institute, 2018) <https://afr.south-wales.police.uk/wp-content/uploads/2019/10/AFR-EVALUATION-REPORT-FINAL-SEPTEMBER-2018.pdf> [accessed 13 July 2022]

Davis, Angela Yvonne, *Are Prisons Obsolete?*, Open Media Book (New York: Seven Stories Press, 2003)

Digital Regulation Cooperation Forum, *Auditing Algorithms: The Existing Landscape, Role of Regulators and Future Outlook* (28 April 2022) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1071554/DRCF_Algorithmic_audit.pdf> [accessed 13 July 2022]

Dodd, Vikram, 'Police Resources "Drained to Dangerously Low Levels", Say Former Top Officers', *The Guardian* (5 July 2019) <https://www.theguardian.com/uk-news/2019/jul/04/police-watchdog-reforms-chief-inspector-constabulary> [accessed 12 July 2022]

Dwyer, Danielle, Wesley Johnson, with PA, 'Police Apologise over CCTV in Muslim Areas', *The Independent* (30 September 2010) <https://www.independent.co.uk/news/uk/crime/police-apologise-over-cctv-in-muslim-areas-2094167.html> [accessed 12 July 2022]

Ephgrave, Nicholas, 'MPS Response to the London Policing Ethics Panel Final Report on Live Facial Recognition Technology' (23 January 2020) <http://www.policingethicspanel.london/uploads/4/4/0/7/44076193/met_response_to_lpep_live_facial_recognition_report.pdf> [accessed 13 July 2022]

Ethnicity Facts and Figures, 'Stop and Search', *Gov.uk* (27 May 2022) <https://www.ethnicity-facts-figures.service.gov.uk/crime-justice-and-the-law/policing/stop-and-search/latest> [accessed 12 July 2022]

European Commission, *Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) And Amending Certain Union Legislative Acts*, COM/2021/206 final (21 April 2021) <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206> [accessed 17 July 2022]

European Court of Human Rights, *Guide on Article 10 of the European Convention on Human Rights – Freedom of Expression* (30 April 2021) <https://www.echr.coe.int/documents/guide_art_10_eng.pdf> [accessed 14 July 2022]

———, *Guide on Article 8 of the European Convention on Human Rights – Right to Respect for Private and Family Life, Home and Correspondence* (31 August 2021) <https://www.echr.coe.int/documents/guide_art_8_eng.pdf> [accessed 14 July 2022]

———, *Guide on Article 11 of the European Convention on Human Rights – Freedom of Assembly and Association* (30 April 2022) <https://www.echr.coe.int/Documents/Guide_Art_11_ENG.pdf> [accessed 14 July 2022]

European Data Protection Supervisor, *Assessing the Necessity of Measures that Limit the Fundamental Right to the Protection of Personal Data: A Toolkit* (11 April 2017) <https://edps.europa.eu/sites/edp/files/publication/17-06-01_necessity_toolkit_final_en.pdf> [accessed 14 July 2022]

———, *Guidelines on Assessing the Proportionality of Measures that Limit the Fundamental Rights to Privacy and to the Protection of Personal Data* (19 December 2019) <https://edps.europa.eu/sites/default/files/publication/19-12-19_edps_proportionality_guidelines2_en.pdf> [accessed 13 July 2022]

European Digital Rights, Access Now, Panoptykon Foundation, epicenter.works, AlgorithmWatch, European Disability Forum, Bits of Freedom, Fair Trials, PICUM, and ANEC (European Consumer Voice in Standardisation), *An EU Artificial Intelligence Act for Fundamental Rights: A Civil Society Statement* (30 November 2021) <https://edri.org/wp-content/uploads/2021/12/Political-statement-on-AI-Act.pdf> [accessed 14 July]

European Parliament, Committee on Civil Liberties, Justice and Home Affairs, *Report on Artificial Intelligence in Criminal Law and its Use by the Police and Judicial Authorities in Criminal Matters*, 2020/2016(INI) (13 July 2021) <https://www.europarl.europa.eu/doceo/document/A-9-2021-0232_EN.html> [accessed 12 July 2022]

Fussey, Pete, and Daragh Murray, *Independent Report on the London Metropolitan Police Service's Trial of Live Facial Recognition Technology*, The Human Rights, Big Data and Technology Project (University of Essex, July 2019) <http://repository.essex.ac.uk/24946/1/London-Met-Police-Trial-of-Facial-Recognition-Tech-Report-2.pdf> [accessed 12 July 2022]

———, 'Policing Uses of Live Facial Recognition in the United Kingdom', in *Regulating Biometrics: Global Approaches and Urgent Questions*, ed. by Amba Kak (New York: AI Now Institute, 2020), pp. 78–85 <https://ainowinstitute.org/regulatingbiometrics-fussey-murray.pdf> [accessed 13 July 2022]

Fussey, Pete, Bethan Davies, and Martin Innes, '"Assisted" Facial Recognition and the Reinvention of Suspicion and Discretion in Digital Policing', *British Journal of Criminology*, 61.2 (2020), 325–44 <https://doi.org/10.1093/bjc/azaa068>

Fussey, Pete, Daragh Murray, and Amy Stevens, 'Written Evidence Submitted to the Justice and Home Affairs Committee', *New Technologies and the Applications of the Law*, NTL0017 (21 October 2021) <https://committees.parliament.uk/writtenevidence/38635/html/> [accessed 13 July 2022]

Galopin, Bernie, and Nigel Nelson, 'Live Facial Recognition, (LFR) MPS Legal Mandate' (23 July 2019) <https://www.statewatch.org/media/documents/news/2018/dec/uk-live-facial-recognition-lfr-mps-legal-mandate.pdf> [accessed 13 July 2022]

Garvie, Clare, 'Garbage In, Garbage Out: Face Recognition on Flawed Data' (Georgetown: Centre on Privacy & Technology, 16 May 2019) <https://www.flawedfacedata.com/> [accessed 13 July]

Greer, Steven, *The Exceptions to Articles 8 and 11 of the European Convention on Human Rights*, Human Rights Files, 15 (Strasbourg: Council of Europe, 1997) <https://www.echr.coe.int/LibraryDocs/DG2/HRFILES/DG2-EN-HRFILES-15(1997).pdf> [accessed 13 July 2022]

Grimond, Will, and Asheem Singh, *A Force for Good? Results from FOI Requests on Artificial Intelligence in the Police Force* (RSA, April 2020) <https://www.thersa.org/globalassets/reports/2020/a-force-for-good-police-ai.pdf> [accessed 12 July 2022]

Grother, Patrick, Mei Ngan, and Kayee Hanaoka, 'Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects', National Institute of Standards and Technology Interagency or Internal Report, 8280 (December 2019) <https://doi.org/10.6028/NIST.IR.8280>

Gwent Police, 'Response to Freedom of Information Request 2022/25016 – Facial Recognition Technology' <https://www.gwent.police.uk/foi-ai/gwent-police/disclosure2/2022/04---april/202225016---facial-recognition-technology/> [accessed 13 July 2022]

Hallowell, Nina, Louise Amoore, Simon Caney, and Peter Waggett, *Ethical Issues Arising from the Police Use of Live Facial Recognition Technology: Interim Report of the Biometrics and Forensics Ethics Group Facial Recognition Working Group* (February 2019) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/781745/Facial_Recognition_Briefing_BFEG_February_2019.pdf> [accessed 14 July 2022]

Hill, Kashmir, 'Wrongfully Accused by an Algorithm', *New York Times* (24 June 2020) <https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html> [accessed 13 July 2022]

HL Deb, 2 February 2022, c983 <https://www.theyworkforyou.com/lords/?id=2022-02-02a.983.0> [accessed 13 July 2022].

Home Office, *Review of the Use and Retention of Custody Images* (February 2017) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/594463/2017-02-23_Custody_Image_Review.pdf> [accessed 14 July 2022]

———, *Surveillance Camera Code of Practice* (November 2021) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1035067/Surveillance_Camera_CoP_Accessible_PDF.pdf> [accessed 13 July 2022]

Home Office News Team, 'Fact Sheet on Live Facial Recognition Used by Police' (4 September 2019) <https://homeofficemedia.blog.gov.uk/2019/09/04/fact-sheet-on-live-facial-recognition-used-by-police/> [accessed 12 July 2022]

House of Commons, Foreign Affairs Committee, *Never Again: The UK's Responsibility to Act on Atrocities in Xinjiang and Beyond*, 2nd Report of Session 2021–22, HC, 198 (8 July 2021) <https://committees.parliament.uk/publications/6624/documents/71430/default/> [accessed 12 July 2022]

House of Lords, Justice and Home Affairs Committee, *Technology Rules? The Advent of New Technologies in the Justice System*, 1st Report of Session 2021–22, HL Paper, 180 (March 2022) <https://committees.parliament.uk/publications/9453/documents/163029/default/> [accessed 12 July 2022]

Independent Office for Police Conduct, *Operation Hotton, Learning Report* (1 February 2022) <https://www.policeconduct.gov.uk/sites/default/files/Operation%20Hotton%20Learning%20report%20-%20January%202022.pdf> [accessed 12 July 2022]

Information Commissioner's Office, 'The Right to Rectification' <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-le-processing/individual-rights/the-right-to-rectification/> [accessed 15 July 2022]

———, *Guidance on the AI Auditing Framework: Draft Guidance for Consultation* (14 February 2020) <https://ico.org.uk/media/2617219/guidance-on-the-ai-auditing-framework-draft-for-consultation.pdf> [accessed 13 July]

———, *Guide to Law Enforcement Processing* (1 January 2021) <https://ico.org.uk/media/for-organisations/guide-to-data-protection/guide-to-le-processing-1-1.pdf> [accessed 14 July 2022]

———, *Information Commissioner's Opinion: The Use of Live Facial Recognition Technology by Law Enforcement in Public Places*, ref. 2019/01 (31 October 2019) <https://ico.org.uk/media/about-the-ico/documents/2616184/live-frt-law-enforcement-opinion-20191031.pdf> [accessed 14 July 2022]

———, *Information Commissioner's Opinion: The Use of Live Facial Recognition Technology in Public Places* (18 June 2021) <https://ico.org.uk/media/2619985/ico-opinion-the-use-of-lfr-in-public-places-20210618.pdf> [accessed 13 July 2022]

Jefferson, Tony, 'Policing the Riots: From Bristol and Brixton to Tottenham, via Toxteth, Handsworth, etc.', *Criminal Justice Matters*, 87 (2012), 8–9 <https://doi.org/10.1080/09627251.2012.670995>

'Jennifer Lee on Privacy, Surveillance and Civil Rights', *The Good Robot* (University of Cambridge Centre for Gender Studies, 7 September 2021) <https://www.buzzsprout.com/1786427/9146359-jennifer-lee-on-privacy-surveillance-and-civil-rights> [accessed 13 July 2022]

Lammy, David, *The Lammy Review Final Report: An Independent Review into the Treatment of, and Outcomes for, Black, Asian and Minority Ethnic Individuals in the Criminal Justice System* (8 September 2017) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/643001/lammy-review-final-report.pdf> [accessed 12 July 2022]

Lewis, Paul, Tim Newburn, Matthew Taylor, Catriona Mcgillivray, Aster Greenhill, Harold Frayman, and Rob Proctor, *Reading the Riots: Investigating England's Summer of Disorder* (London: London School of Economics and Political Science and *The Guardian*, 2011) <http://eprints.lse.ac.uk/46297/1/Reading%20the%20riots(published).pdf> [accessed 12 July 2022]

Lewis, Tamika, Seeta Peña Gangadharan, Mariella Saba, and Tawana Petty, *Digital Defense Playbook: Community Power Tools for Reclaiming Data* (Detroit: Our Data Bodies, 2018) <https://www.odbproject.org/wp-content/uploads/2019/03/ODB_DDP_HighRes_Spreads.pdf> [accessed 12 July 2022]

Liberty, 'Briefing on the Amended Surveillance Camera Code of Practice' (January 2022) <https://www.libertyhumanrights.org.uk/wp-content/uploads/2022/01/Libertys-briefing-on-the-amended-Surveillance-Camera-Code-of-Practice-January-2022.pdf> [accessed 12 July 2022]

Livingstone, Adele, 'Humberside Police Information Compliance, Response to Freedom of Information Request: Facial Recognition Used on [the] 13th and 14th June 2018 at King George Docks, ref: F-2018-01559' (6 August 2018) <https://www.whatdotheyknow.com/request/facial_recognition_used_on_the_t> [accessed 14 July 2022]

London Policing Ethics Panel, 'Minutes of Meeting, 12 February 2018' <http://www.policingethicspanel.london/uploads/4/4/0/7/44076193/lpep_minutes_12_february_2018.pdf> [accessed 15 July 2022]

———, ‘Minutes of Meeting, 14 May 2018’ <http://www.policingethicspanel.london/uploads/4/4/0/7/44076193/2018_05_14_lpep_minutes_14_may_2018.pdf> [accessed 15 July 2022]

———, ‘Minutes of Meeting, 11 June 2018' <http://www.policingethicspanel.london/uploads/4/4/0/7/44076193/2018_06_11_lpep_minutes_11_june_2018.pdf> [accessed 15 July 2022]

———, ‘Minutes of Meeting, 9 July 2018’ <http://www.policingethicspanel.london/uploads/4/4/0/7/44076193/lpep_minutes_9_july_2018.pdf> [accessed 15 July 2022]

———, ‘Interim Report on Live Facial Recognition’ (July 2018) <http://www.policingethicspanel.london/uploads/4/4/0/7/44076193/lpep_report_-_live_facial_recognition.pdf> [accessed 15 July 2022]

———, ‘Final Report on Live Facial Recognition’ (May 2019) <http://www.policingethicspanel.london/uploads/4/4/0/7/44076193/live_facial_recognition_final_report_may_2019.pdf> [accessed 15 July 2022]

Mayor of London, Mayor’s Office for Policing and Crime, ‘London Policing Ethics Panel Terms of Reference’ <http://www.policingethicspanel.london/uploads/4/4/0/7/44076193/london_policing_ethics_panel_terms_of_reference_2017.pdf> [accessed 15 July 2022]

———, ‘MOPAC Decisions: Retrospective Facial Recognition System’ (19 August 2021) <https://www.london.gov.uk/what-we-do/mayors-office-policing-and-crime-mopac/governance-and-decision-making/mopac-decisions-0/retrospective-facial-recognition-system> [accessed 14 July]

———, Metropolitan Police Service, ‘Accessibility’ <https://www.met.police.uk/hyg/accessibility/> [accessed 17 July 2022]

———, ‘Equality Impact Assessment’ <https://www.met.police.uk/SysSiteAssets/media/downloads/force-content/met/advice/lfr/impact-assessments/lfr-eia.pdf> [accessed 13 July 2022]

———, ‘Facial Recognition’ <https://www.met.police.uk/advice/advice-and-information/fr/facial-recognition/> [accessed 14 July 2022]

———, ‘MPS LFR Deployments 2020 – Date’ <https://www.met.police.uk/SysSiteAssets/media/downloads/force-content/met/advice/lfr/deployment-records/lfr-deployment-grid.pdf> [accessed 14 July 2022]

———, ‘Response to Freedom of Information Request: MPS’s Trial of Live Facial Recognition

———, Technology, ref. 01.FOI.19.011245’ <https://www.met.police.uk/foi-ai/metropolitan-police/disclosure-2019/september/mps-trial-live-facial-recognition-technology/> [accessed 15 July 2022]

———, ‘Community Impact Assessment: Op Fahrenheit – MPS Live Facial Recognition’ (11 February 2020) <https://www.met.police.uk/SysSiteAssets/foi-media/metropolitan-police/disclosure_2020/august_2020/live-facial-recognition-technology-att2.pdf> [accessed 15 July 2022]

———, ‘Appropriate Policy Document for Sensitive Data Processing Within Live Facial Recognition Deployments’ (10 February 2021) <https://www.met.police.uk/SysSiteAssets/media/downloads/central/services/accessing-information/facial-recognition/appropriate-policy-document.pdf> [accessed 15 July 2022]

———, ‘Live Facial Recognition: Legal Mandate’ (29 November 2022) <https://www.met.police.uk/SysSiteAssets/media/downloads/force-content/met/advice/lfr/policy-documents/lfr-legal-mandate.pdf> [accessed 12 July 2022]

Metropolitan Police Service, Information Rights Unit, ‘Response to Freedom of Information Request: Live Facial Recognition Deployments, ref. 01FOI/22/024489’ (4 June 2022) <https://drive.google.com/file/d/1xl7W5ZDopekq-gVzwjZysiOtgiBYttuz/view?usp=sharing> [accessed 15 July 2022]

———, ‘Response to Freedom of Information Request: MPS’ Use of Live Facial Recognition, ref. 01FOI/22/024139’ (17 June 2022) <https://drive.google.com/file/d/1wEk-2FVtUGetiaKsOa1HGTZ9qQ4XNa1B/view?usp=sharing> [accessed 15 July 2022]

Michael, Alun, *Police and Crime Commissioner for South Wales/De Cymru Comisiynydd yr Heddlu a Throseddu: Annual Report*, 2015–2016 <http://pcclivewww.blob.core.windows.net/wordpress-uploads/2151-SWPCC-Annual-Report-2015-2016-English.pdf> [accessed 14 July 2022]

Morris, Steven, ‘Response to Freedom of Information Request: Leicestershire Police Using Biometric Facial Recognition Technology – NeoFace, ref: 008302/14’ (15 January 2015) <https://www.whatdotheyknow.com/request/240739/response/605917/attach/html/2/8302%2014.pdf.html> [accessed 14 July 2022]

Moss, Emanuel, Elizabeth Anne Watkins, Ranjit Singh, Madeleine Clare Elish, and Jacob Metcalf, *Assembling Accountability: Algorithmic Impact Assessment for the Public Interest* (Data & Society, 29 June 2021) <http://dx.doi.org/10.2139/ssrn.3877437>

National Physical Laboratory and Metropolitan Police Service, *Metropolitan Police Service Live Facial Recognition Trials*: *Trials Period August 2016–February 2019* (February 2020) <https://www.met.police.uk/syssiteassets/media/downloads/central/services/accessing-information/facial-recognition/met-evaluation-report.pdf> [accessed 12 July 2022]

'NEC Corp', *Investigate: A Project of the American Friends Service Committee* (25 October 2021) <https://investigate.afsc.org/company/nec> [accessed 13 July 2022]

Nelson, Nigel, 'Metropolitan Police Service Privacy Impact Assessment' (25 July 2019) <https://www.statewatch.org/media/documents/news/2018/dec/uk-metropolitan-police-service-privacy-impact-assessment-lfr.pdf> [accessed 13 July 2022]

Nicas, Jack, 'Atlanta Asks Google Whether It Targeted Black Homeless People', *New York Times* (4 October 2019) <https://www.nytimes.com/2019/10/04/technology/google-facial-recognition-atlanta-homeless.html> [accessed 13 July 2022]

Oswald, Marion, 'A Three-Pillar Approach to Achieving Trustworthy and Accountable Use of AI and Emerging Technology in Policing in England and Wales: Lessons from the West Midlands Data Ethics Model', *European Journal of Law and Technology*, 13.1 (2022) <https://ejlt.org/index.php/ejlt/article/view/883/1045> [accessed 14 July 2022]

Oswald, Marion, and Sheena Unwin, 'Written Evidence Submitted to the House of Lords, Science and Technology Committee', *Algorithms in Decision-Making*, ALG0030 (23 May 2018) <http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/science-and-technology-committee/algorithms-in-decisionmaking/written/69002.html> [accessed 13 July 2022]

Porter, Anthony, *Facing the Camera: Good Practice and Guidance for the Police Use of Overt Surveillance Camera Systems Incorporating Facial Recognition Technology to Locate Persons on a Watchlist, in Public Places in England & Wales* (November 2020) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/940386/6.7024_SCC_Facial_recognition_report_v3_WEB.pdf> [accessed 13 July 2022]

Privacy International, 'Digital Stop and Search: How the UK Police Can Secretly Download Everything from Your Mobile Phone' (March 2018) <https://privacyinternational.org/sites/default/files/2018-03/Digital%20Stop%20and%20Search%20Report.pdf> [accessed 14 July 2022]

———, 'Submission to the Scottish Parliament's Justice Sub-Committee on Policing's Inquiry into Facial Recognition Policing' (November 2019) <https://privacyinternational.org/sites/default/files/2020-04/19.11.01_JusticeSC_FRT_Evidence_PI_FINAL_2%20%282%29.pdf> [accessed 14 July 2022]

Privacy International, Liberty, Defend Digital Me, Open Rights Group, and Big Brother Watch, 'Consultation on Live Facial Recognition APP. Feedback Form' (27 June 2021) <https://privacyinternational.org/sites/default/files/2021-06/LFRT%20Consultation%20Response%20Final_0.pdf> [accessed 12 July 2022]

Purshouse, Joe, and Liz Campbell, 'Automated Facial Recognition and Policing: A Bridge Too Far?', *Legal Studies*, 42.2 (2022), 209–227 <https://doi.org/10.1017/lst.2021.22>

Pyper, Doug, 'The Public Sector Equality Duty and Equality Impact Assessments', *House of Commons Library Briefing Paper*, 06591 (8 July 2020) <https://researchbriefings.files.parliament.uk/documents/SN06591/SN06591.pdf> [accessed 13 July]

R (Bridges) v. Chief Constable of South Wales Police, Judgement, High Court, Queen's Bench Division, case CO/4085/2018 (4 September 2019) <https://www.judiciary.uk/wp-content/uploads/2019/09/bridges-swp-judgment-Final03-09-19-1.pdf> [accessed 14 July 2022]

R (Bridges) v. Chief Constable of South Wales Police, Judgement, Court of Appeal, Civil Division, case C1/2019/2670 (11 August 2020) <https://www.judiciary.uk/wp-content/uploads/2020/08/R-Bridges-v-CC-South-Wales-ors-Judgment.pdf> [accessed 13 July 2022]

Raji, Inioluwa Deborah, and Joy Buolamwini, 'Actionable Auditing: Investigating the Impact of Publicly Naming Biased Performance Results of Commercial AI Products', *Conference on Artificial Intelligence, Ethics, and Society* (2019) <https://www.thetalkingmachines.com/sites/default/files/2019-02/aies-19_paper_223.pdf> [accessed 13 July 2022]

Raji, Inioluwa Deborah, Timnit Gebru, Margaret Mitchell, Joy Buolamwini, Joonseok Lee, and Emily Denton, 'Saving Face: Investigating the Ethical Concerns of Facial Recognition Auditing', *AAI/ACM Conference on Artificial Intelligence, Ethics, and Society* (2020), 145–51 <https://doi.org/10.1145/3375627.3375820>

Rees, Jenny, 'Facial Recognition Use by South Wales Police Ruled Unlawful', *BBC Wales* <https://www.bbc.co.uk/news/uk-wales-53734716> [accessed 13 July 2022]

RMC and FJ v. Commissioner of Police for the Metropolis and Secretary of State for the Home Department, Judgement, High Court, Queen's Bench Division, cases CO/12476/2010 and CO/5572/2011 (22 June 2012) <https://www.judiciary.uk/wp-content/uploads/JCO/Documents/Judgments/r-rmc-fj-metropolitan-police-commissioner-22062012.pdf> [accessed 13 July 2022]

Robson, Steve, 'Greater Manchester Police Monitored Every Visitor to Trafford Centre for SIX MONTHS Using Controversial Technology Until They Were Told to Stop', *Manchester Evening News* (14 October 2018) <https://www.manchestereveningnews.co.uk/news/greater-manchester-news/gmp-trafford-centre-camera-monitored-15278943> [accessed 14 July 2022]

Ryan, Joe, 'Reports of Misogyny and Sexual Harassment in the Metropolitan Police', *House of Commons Library Debate Pack*, CDP 2022/0046 (1 March 2022) <https://researchbriefings.files.parliament.uk/documents/CDP-2022-0046/CDP-2022-0046.pdf> [accessed 12 July 2022]

Ryder, Matthew, *The Ryder Review: Independent Legal Review of the Governance of Biometric Data in England and Wales* (Ada Lovelace Institute, June 2022) <https://www.adalovelaceinstitute.org/wp-content/uploads/2022/06/The-Ryder-Review-Independent-legal-review-of-the-governance-of-biometric-data-in-England-and-Wales-Ada-Lovelace-Institute-June-2022.pdf> [accessed 12 July 2022]

S. and Marper v. United Kingdom, Judgement, ECtHR 1581, app. nos 30562/04, 30566/04 (4 December 2008) <https://www.bailii.org/eu/cases/ECHR/2008/1581.html> [accessed 14 July 2022]

Sampson, Fraser, 'Letter from the Biometrics and Surveillance Camera Commissioner to the Secretary of State for Levelling Up, Housing and Communities', *Gov.uk* (22 April 2022) <https://www.gov.uk/government/publications/letters-from-the-biometrics-and-surveillance-camera-commissioner-april-2022/letter-from-the-biometrics-and-surveillance-camera-commissioner-to-the-secretary-of-state-for-levelling-up-housing-and-communities-22-april-2022-acc> [accessed 12 July 2022]

———, 'The Biometrics and Surveillance Cameras Commissioner's Response to the College of Policing APP on Live Facial Recognition', *Gov.uk* (6 April 2022) <https://www.gov.uk/government/news/the-biometrics-and-surveillance-camera-commissioners-response-to-the-college-of-policing-app-on-live-facial-recognition> [accessed 12 July 2022]

Scottish Parliament, Justice Sub-Committee on Policing, *Facial Recognition: How Policing in Scotland Makes Use of This Technology*, 1st Report, 2020 (Session 5), SP, 678 (11 February 2020) <https://sp-bpr-en-prod-cdnep.azureedge.net/published/JSP/2020/2/11/Facial-recognition--how-policing-in-Scotland-makes-use-of-this-technology/JSPS0520R01.pdf> [accessed 13 July 2022]

Solon, Olivia, 'Facial Recognition's "Dirty Little Secret": Millions of Online Photos Scrapes Without Consent', *NBC News* (17 March 2019) <https://www.nbcnews.com/tech/internet/facial-recognition-s-dirty-little-secret-millions-online-photos-scraped-n981921> [accessed 12 July 2022]

South Wales Police, 'Accessibility' <https://www.south-wales.police.uk/hyg/accessibility/> [accessed 16 July 2022]

———, 'Data Protection Impact Assessment for Live Facial Recognition (LFR)' <https://www.south-wales.police.uk/SysSiteAssets/media/downloads/south-wales/about-us/live-facial-recognition/lfr-dpia-v0.4.pdf> [accessed 17 July 2022]

———, 'Facial Recognition Technology' <https://www.south-wales.police.uk/police-forces/south-wales-police/areas/about-us/about-us/facial-recognition-technology/> [accessed 14 July 2022]

———, 'List of Previous FRT Deployments' <https://www.south-wales.police.uk/SysSiteAssets/media/downloads/south-wales/about-us/frt/FRT-deployments.pdf> [accessed 12 July 2022]

———, 'Operator Initiated Facial Recognition Documents' <https://www.south-wales.police.uk/police-forces/south-wales-police/areas/about-us/about-us/facial-recognition-technology/operator-initiated-facial-recognition-documents/> [accessed 13 July 2022]

———, 'Our Vision, Values, and Ethics' <https://www.south-wales.police.uk/police-forces/south-wales-police/areas/about-us/about-us/our-vision-values-and-ethics/> [accessed 14 July 2022]

———, 'Privacy Notice' <https://www.south-wales.police.uk/hyg/southwales/privacy-notice/> [accessed 17 July 2022]

———, *Smarter Recognition, Safer Community* <https://afr.south-wales.police.uk/smarter-recognition/> [accessed 13 July 2022]

———, 'Data Protection Impact Assessment: Automated Facial Recognition (AFR)' (11 October 2018) <https://afr.south-wales.police.uk/wp-content/uploads/2019/10/DPIA-V5.4-Live.pdf> [accessed 14 July 2022]

———, 'Whistleblowing: Guidance & Procedure Summary' (14 March 2019) <https://www.south-wales.police.uk/SysSiteAssets/media/downloads/south-wales/about-us/policies-and-procedures/english/whistleblowing.pdf> [accessed 14 July 2022]

———, 'Equality Impact Assessment: Facial Recognition Technology – Retrospective, Live and Operator Initiated' (10 August 2021) <https://drive.google.com/file/d/1yuH0e4tsFKDofTz-diloltbVHpOBH3t-/view?usp=sharing> [accessed 13 July 2022]

———, 'New Facial Recognition Mobile App to Identify Vulnerable, Missing and Wanted Individuals' (7 December 2021) <https://www.south-wales.police.uk/news/south-wales/news/2021/december/new-facial-recognition-app-to-to-identify-wanted-individuals/> [accessed 12 July 2022]

———, 'Keeping South Wales Safe with Facial Recognition Technology' (14 March 2022) <https://www.south-wales.police.uk/news/south-wales/news/2022/maw-mar/keeping-south-wales-safe-with-facial-recognition-technology/> [accessed 14 July 2022]

———, 'Facial Recognition App Pilot Results' (29 April 2022) <https://www.south-wales.police.uk/news/south-wales/news/2022/ebr-apr/pilot-results-for-the-new-facial-recognition-app/> [accessed 13 July 2022]

South Wales Police and Gwent Police, 'Data Protection Impact Assessment for Operator Initiated Facial Recognition (OIFR)' <https://www.south-wales.police.uk/SysSiteAssets/media/downloads/south-wales/about-us/frt/oifr-documents/oifr-dpia-v0.5.pdf> [accessed 15 July 2022]

———, 'Operator Initiated Facial Recognition (OIFR) Legal Mandate' (25 January 2022) <https://www.south-wales.police.uk/SysSiteAssets/media/downloads/south-wales/about-us/frt/oifr-documents/oifr-legal-mandate-v0.4.pdf> [accessed 15 July 2022]

———, 'Policy Document for the Overt Use of Operator Initiated Facial Recognition (OIFR)' (25 January 2022) <https://www.south-wales.police.uk/SysSiteAssets/media/downloads/south-wales/about-us/frt/oifr-documents/oifr-policy-v0.4.pdf> [accessed 17 July 2022]

———, 'Standard Operating Procedures for the Overt Use of Operator Initiated Facial Recognition (OIFR)' (25 January 2022) <https://www.south-wales.police.uk/SysSiteAssets/media/downloads/south-wales/about-us/frt/oifr-documents/oifr-sop-v0.6.pdf> [accessed 17 July 2022]

South Wales Police and Crime Commissioner and Chief Constable, 'Person Specification – Independent Ethics Committee' (2017) <https://www.south-wales.police.uk/SysSiteAssets/media/downloads/south-wales/about-us/careers/hr-documents/person-specification-2020.pdf> [accessed 15 July 2022]

———, 'Appointment of Members to *The Independent* Ethics Committee' (July 2022) <https://www.south-wales.police.uk/SysSiteAssets/media/downloads/south-wales/about-us/careers/hr-documents/job-description-june-22-update.pdf> [accessed 15 July 2022]

South Wales Police Corporate Services, *Briefing Pack: Independent Ethics Committee Members* (May 2022) <https://www.south-wales.police.uk/SysSiteAssets/media/downloads/south-wales/about-us/careers/hr-documents/2022-06-08-iec-information-pack-new.pdf> [accessed 15 July 2022]

South Wales Police Joint Independent Ethics Committee, 'Meeting Minutes, 12 September 2018' <https://www.south-wales.police.uk/SysSiteAssets/media/downloads/force-content/south-wales/independent-ethics-committee/independent-ethics-committee-meeting-minutes-october-2018.pdf> [accessed 14 July 2022]

———, 'Meeting Minutes, 12 December 2018' <https://www.south-wales.police.uk/SysSiteAssets/media/downloads/force-content/south-wales/independent-ethics-committee/independent-ethics-committee-meeting-minutes-december-2018.pdf> [accessed 14 July 2022]

———, 'Meeting Minutes, 27 March 2019' <https://www.south-wales.police.uk/SysSiteAssets/media/downloads/force-content/south-wales/independent-ethics-committee/independent-ethics-committee-meeting-minutes-March-2019.docx> [accessed 14 July 2022]

———, 'Meeting Minutes, 10 June 2021' <https://www.south-wales.police.uk/SysSiteAssets/media/images/south-wales/about-us/stats-and-data/joint-independent-ethics-committee-minutes---june-2021.pdf> [accessed 17 July 2022]

South Wales Police Twitter Account, @swpolice, tweet (8 December 2021)

Talora, Joe, 'No Anonymity for Met Police Whistleblowers, Says Deputy Commissioner Sir Stephen House', *Evening Standard* (17 November 2021) <https://www.standard.co.uk/news/london/met-police-misconduct-no-anonymity-whistleblowers-deputy-commissioner-stephen-house-b966743.html> [accessed 15 July 2022]

———, 'Met Police Whistleblowers Need Anonymity to Tackle "Culture of Silence", Says Top London Tory' (3 February 2022) <https://www.standard.co.uk/news/london/metropolitan-police-cressida-dick-misconduct-iopc-london-tory-susan-hall-b980408.html> [accessed 15 July 2022]

Tele2 Sverige AB v. Post-och telestyrelsen and Secretary of State for the Home Department v. Watson and others, Judgement, Grand Chamber, Court of Justice of the European Union, cases C-203/15, C-698/15 (21 December 2016) <https://curia.europa.eu/juris/document/document.jsf?text=&docid=186492&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=1088733> [accessed 14 July 2022]

Townsend, Mark, 'Police to Use Facial-Recognition Cameras at Cenotaph Service', *The Observer* (12 November 2017) <https://www.theguardian.com/technology/2017/nov/12/metropolitan-police-to-use-facial-recognition-technology-remembrance-sunday-cenotaph> [accessed 12 July 2022]

TRUST San Diego Coalition, 'City of San Diego, Proposed Surveillance Ordinance and Privacy Commission' <https://sandiegotrust.org/City_of_San_Diego_Proposed_Surveillance_Ordinance_and_Privacy_Commission.pdf> [accessed 14 July 2022]

United Nations, Office of the High Commissioner for Human Rights, 'Artificial Intelligence Risks to Privacy Demand Urgent Action – Bachelet', *Press Releases* (15 September 2021) <https://www.ohchr.org/en/2021/09/artificial-intelligence-risks-privacy-demand-urgent-action-bachelet> [accessed 12 July 2022]

United Nations High Commissioner for Human Rights, *Impact of New Technologies on the Promotion and Protection of Human Rights in the Context of Assemblies, Including Peaceful Protests - Report*, Human Rights Council, 44th session, 15 June–3 July 2020, Agenda items 2 and 3, A/HRC/44/24 (24 June 2020) <https://www.ohchr.org/sites/default/files/HRBodies/HRC/RegularSessions/Session44/Documents/A_HRC_44_24_AEV.docx> [accessed 14 July 2022]

Vitale, Alex S., *The End of Policing* (London: Verso, 2017)

Weale, Sally, 'ICO to Step in After Schools Use Facial Recognition to Speed Up Lunch Queue', *The Guardian* (18 October 2021) <https://www.theguardian.com/education/2021/oct/18/privacy-fears-as-schools-use-facial-recognition-to-speed-up-lunch-queue-ayrshire-technology-payments-uk> [accessed 14 July 2022]

West Midlands Police and Crime Commissioner, 'West Midlands Police's Ethics Committee: Terms of Reference' (July 2019) <https://www.westmidlands-pcc.gov.uk/wp-content/uploads/2019/07/Ethics-Committee-Terms-of-Reference-as-at-1-April-2019.pdf?x39505> [accessed 14 July 2022]

Wiles, Paul, 'Biometrics Commissioner on the Police Use of Live Facial Recognition', *Gov.uk* (11 February 2020) <https://www.gov.uk/government/news/biometrics-commissioner-on-the-police-use-of-live-facial-recognition> [accessed 12 July 2022]

Williams, Patrick, *Being Matrixed: The (Over)Policing of Gang Suspects in London* (StopWatch, August 2018) <https://www.stop-watch.org/what-we-do/research/being-matrixed-the-overpolicing-of-gang-suspects-in-london/> [accessed 12 July 2022]

Williams, Rhiannon, 'Police Across UK Testing New Retrospective Facial Recognition that Could Identify Criminals and Missing People', *i News* (31 July 2021) <https://inews.co.uk/news/technology/uk-police-testing-retrospective-facial-recognition-identify-criminals-1128711> [accessed 14 July 2022]

Winchester, Nicole, 'Covid-19 and the Police: New Powers but More Pressure?', *House of Lords Library*, In Focus (27 March 2020) <https://lordslibrary.parliament.uk/covid-19-and-the-police-new-powers-but-more-pressure/> [accessed 12 July 2022]

Woods, Lorna, 'United Kingdom – Automated Facial Recognition in the UK: The *Bridges* Case and Beyond', *European Data Protection Law Review*, 6.3 (2020), 455–463 <https://doi.org/10.21552/edpl/2020/3/16>.

APPENDIX

A. Cases of Police Use of Facial Recognition in England and Wales

Below we share known cases of police use of facial recognition in England and Wales. More than 10 police forces have deployed facial recognition, starting as early as 2014. Note that the Metropolitan Police Service and South Wales Police paused their live FRT deployments due to the COVID-19 pandemic and resumed them in 2022. Deployments of live FRT are highlighted in blue, retrospective FRT in red, and operator initiated FRT in lilac.

Police Force	Type of Facial Recognition Technology	Deployment Dates
Leicestershire Police	Retrospective (trial)	Apr 2014 to Jan 2015
Leicestershire Police	Live (trial)	Jun 2015
Metropolitan Police Service	Live (trial)	Aug 2016 to Feb 2019
South Wales Police	Live (trial)	May 2017 to Jan 2020
South Yorkshire Police	Live (trial)	Jan 2018 to Mar 2018
Manchester Police	Live (trial)	Apr 2018 to Sep 2018
Humberside Police	Live (trial)	Jun 2018
South Wales Police	Operator initiated (trial)	Aug 2019 to Oct 2019
All England and Wales forces	Retrospective (via the Police National Database)	Sep 2019 to Present
Metropolitan Police Service	Live	Feb 2020
Hampshire Constabulary	Retrospective (trial)	July 2021 to Present
Humberside Police	Retrospective (trial)	July 2021 to Present
North Wales Police	Retrospective (trial)	July 2021 to Present
South Yorkshire Police	Retrospective (trial)	July 2021 to Present
South Wales Police	Operator initiated (trial)	Dec 2021 to Mar 2022
Metropolitan Police Service	Live	Jan 2022 to Present
South Wales Police	Live (trial)	Mar 2022 to Present
Cheshire Constabulary	Retrospective (trial)	Apr 2022 to Present
Cheshire Constabulary	Operator initiated (trial)	Jun 2022 to Present
Metropolitan Police Service	Retrospective	Will be used soon

B. Terminology for Audit Questions

Below we provide definitions for terms used in the audit scorecard in **Section 6**.

Term	Definition
Chilling effect	A discouraging effect on the exercise of fundamental rights, such as freedom of peaceful assembly, as a result of police use of FRT.
Clear, objective, and limited criteria	Criteria that are published and understandable ('accessible') and do not leave too broad of a discretion to police officers ('foreseeable'). This is mandated by the 'in accordance with the law' requirement to protect against arbitrary interference with Article 8 privacy rights of the Human Rights Act 1998.
Demographic	Relating to the characteristics of a population such as race, gender, or age.
Function creep	The widening of the use of FRT beyond its originally specified purposes.
Marginalised communities	Communities that face discrimination and exclusion from society, politics, and the economy. In the context of police use of FRT, marginalised communities include groups historically subject to disproportionate surveillance and policing practices. In England and Wales, marginalised communities include but are not limited to: people of colour, immigrant populations, low-income communities, religious minorities, people with disabilities, and Gypsy, Roma, and Traveller groups.
Police	One of the police forces in England and Wales being evaluated by the audit.
Police organisation	A public organisation of police service. In England and Wales, police organisations include police forces, the National Crime Agency, the National Police Chiefs' Council, and the College of Policing.
Probe image	An unknown facial image that is searched against a watchlist.
Procedurally fair	Having a fair process when making a decision. The following are examples of what may be needed to ensure procedural fairness: a sufficient notice to participate in the process, the opportunity to be heard by an unbiased decision-maker, and a process to appeal the decision.
Type of FRT	The category of FRT being used by the police force. Types of FRT include live, retrospective, and mobile phone FRT.
Watchlist	A set of known facial images against which a probe image is searched. The watchlist is also referred to as the image reference database.
Where and when FRT can be used	The circumstances in which FRT can be used, including factors such as the police intelligence case and the location where the probe image is captured. For live FRT and mobile phone FRT, this location refers to the place where FRT is deployed. For retrospective FRT, this location refers to the place where the probe image is taken, rather than the place where FRT is applied to the image at a later point in time.

C. Sources for Audit Questions

To construct the audit, we reviewed existing literature on police use of FRT in England and Wales and used sources from a variety of perspectives:

- Primary legislation relevant to police use of facial recognition in England and Wales
- **Users:** Documents on facial recognition developed by police forces in England and Wales
- **Courts:** Legal challenges to police use of facial recognition and related court cases
- **Legislators:** Reports developed by UK legislative committees on police use of new technologies
- **Regulators:** Guidance from UK regulatory bodies on facial recognition and legal compliance
- **Academia:** Academic evaluations of police use of FRT in England and Wales
- **Advisors:** Resources developed by oversight or advisory bodies on data and technology usage
- **Auditors:** Evaluations conducted by algorithmic auditors to test facial recognition performance
- **Civil society:** Resources developed by civil society on facial recognition and AI governance

We summarise the sources used from these perspectives in the table below and then detail how specific sources were leveraged to generate each question of the audit. See the **Bibliography** for the full citations of the sources used.

Abbreviation	Resources
Primary legislation relevant to police use of facial recognition in England and Wales	
DPA18	Data Protection Act 2018
GDPR	General Data Protection Regulation
HRA	Human Rights Act 1998
PSED	Public Sector Equality Duty (Section 149 of Equality Act 2010)
Users: Documents on facial recognition developed by police forces in England and Wales	
Police Force Documents	A. Metropolitan Police Service, 'Facial Recognition'. B. South Wales Police, 'Facial Recognition Technology'.
Courts: Legal challenges to police use of facial recognition and related court cases	
Bridges Case	A. *R (Bridges) v. Chief Constable of South Wales Police, Judgement,* Court of Appeal. B. *R (Bridges) v. Chief Constable of South Wales Police, Judgement,* High Court.
Marper Case	*S. and Marper v. United Kingdom.*
RMC Case	*RMC and FJ v. Commissioner of Police for the Metropolis and Secretary of State for the Home Department.*
Watson Case	*Tele2 Sverige AB v. Post-och telestyrelsen and Secretary of State for the Home Department v. Watson and others.*
Legislators: Reports developed by UK legislative committees on police use of new technologies	
House of Lords	House of Lords, Justice and Home Affairs Committee, *Technology Rules?*
Scottish Parliament	Scottish Parliament, Justice Sub-Committee on Policing, *Facial Recognition: How Policing in Scotland Makes Use of This Technology.*

Abbreviation	Resources
Regulators: Guidance from UK regulatory bodies on facial recognition and legal compliance	
ICO	A. Information Commissioner's Office, *Guide to Law Enforcement Processing.* B. Information Commissioner's Office, *Information Commissioner's Opinion: The Use of Live Facial Recognition Technology by Law Enforcement in Public Places.* C. Information Commissioner's Office, *Information Commissioner's Opinion: The Use of Live Facial Recognition Technology in Public Places.*
Academia: Academic evaluations of police use of FRT in England and Wales	
Cardiff Report	Davies, Innes, and Dawson, *An Evaluation of South Wales Police's Use of Automated Facial Recognition*.
Essex Report	Fussey and Murray, *Independent Report*.
Advisors: Resources developed by oversight or advisory bodies on data and technology usage	
BFEG	A. Biometrics and Forensics Ethics Group, *Briefing Note.* B. Hallowell and others, *Ethical Issues Arising from the Police Use of Live Facial Recognition Technology.*
College of Policing	A. College of Policing, 'Intelligence Report'. B. College of Policing, 'Live Facial Recognition'.
ECHR Guidance	A. European Court of Human Rights, *Guide on Article 8.* B. European Court of Human Rights, *Guide on Article 10.* C. European Court of Human Rights, *Guide on Article 11*.
European Data Protection Supervisor	A. European Data Protection Supervisor, *Assessing the Necessity of Measures.* B. European Data Protection Supervisor, *Guidelines on Assessing the Proportionality of Measures.*
Local Oversight	A. TRUST San Diego Coalition, 'City of San Diego, Proposed Surveillance Ordinance and Privacy Commission'. B. West Midlands Police and Crime Commissioner, 'West Midlands Police's Ethics Committee: Terms of Reference'.
Surveillance Camera Guidance	A. Home Office, *Surveillance Camera Code of Practice.* B. Porter, *Facing the Camera.*
UK Cabinet Office	Cabinet Office, 'Consultation Principles: Guidance'.

Abbreviation	Resources
UN Human Rights	United Nations High Commissioner for Human Rights, *Impact of New Technologies on the Promotion and Protection of Human Rights.*
Auditors: Evaluations conducted by algorithmic auditors to test facial recognition performance	
NIST	Grother, Ngan, and Hanaoka, 'Face Recognition Vendor Test'.
Civil society: Resources developed by civil society on facial recognition and AI governance	
Civil Society on FRT	A. Big Brother Watch, *Briefing on Facial Recognition Surveillance.* B. Big Brother Watch and Open Rights Group, 'Joint Submission to the Scottish Parliament Justice Sub-Committee'. C. Chowdhury, *Unmasking Facial Recognition.* D. Liberty, 'Briefing on the Amended Surveillance Camera Code of Practice'. E. Privacy International, 'Submission to the Scottish Parliament's Justice Sub-Committee on Policing's Inquiry into Facial Recognition Policing'. F. Privacy International and others, 'Consultation on Live Facial Recognition APP. Feedback Form'.
Civil Society on Technology	A. American Civil Liberties Union, 'Community Control Over Police Surveillance (CCOPS) Model Bill'. B. American Civil Liberties Union, 'Tech Equity Coalition'. C. Amnesty International, *Trapped in the Matrix.* D. Big Brother Watch, 'Written Evidence for the Justice and Home Affairs Committee's Inquiry into New Technologies'. E. European Digital Rights and others, *An EU Artificial Intelligence Act for Fundamental Rights: A Civil Society Statement.* F. Privacy International, 'Digital Stop and Search'.

C.1 Legal standards

In Accordance with the Law (Human Rights Act 1998)

A. Are there clear, objective, and limited criteria for who can be included in the watchlist, including with regard to the image source and the seriousness of offence or risk?

Source: HRA Article 8(2), *Bridges* Case, ICO, *Watson* Case
To be lawful, FRT's interference with Article 8 privacy rights of the Human Rights Act 1998 must be 'in accordance with the law' and must satisfy the legal tests of necessity and proportionality. For the 'in accordance with the law' requirement to be met, the *Bridges* court case ruled that the criteria for who is included in the watchlist must be clear and not leave too broad a discretion to individual officers. Additionally, the case law of the European Court of Human Rights and the Court of Justice of the European Union, such as the *Watson* court case, has established that covert surveillance may not be justified in relation to all crimes or intelligence activities, and that mass covert surveillance is only justified with regard to serious crime.[116] The ICO guidance has also highlighted the importance of limits on the watchlist criteria with regard to the seriousness of offence: 'Watchlists of individuals suspected of minor offences are less likely to satisfy the key legal tests of necessity and proportionality'.[117]

B. Are there clear, objective, and limited criteria for where and when FRT can be used, including mandating reasonable suspicion that persons on the watchlist will be at the location and requiring a high grade of intelligence for the police intelligence case that supports FRT use?

Source: HRA Article 8(2), *Bridges* Case, College of Policing, ICO
To be lawful, FRT's interference with Article 8 privacy rights of the Human Rights Act 1998 must be 'in accordance with the law' and must satisfy the legal tests of necessity and proportionality. For the 'in accordance with the law' requirement to be met, the *Bridges* court case ruled that the criteria for where FRT is deployed must be clear and not leave too broad a discretion to individual officers. In the case, the Court criticised South Wales Police's broad criteria: 'the range is very broad and without apparent limits. It is not said, for example, that the location must be one at which it is thought on reasonable grounds that people on the watchlist will be present'.[118] The ICO guidance also notes that, 'watchlists comprising images of individuals where there is no reasonable expectation that they will be in the vicinity of the LFR deployment are also less likely to meet [the key legal tests of necessity and proportionality]'.[119] Additionally, to meet these legal tests, the ICO and College of Policing have stressed the importance that deployments are intelligence-led ('where the police have specific intelligence showing that suspects are likely to be present at a particular location at a particular time').[120] However, given that the quality of intelligence can range broadly, mandating a high grade of intelligence is critical. To help police forces apply the national intelligence model, the College of Policing's authorised professional practice (APP) on intelligence management establishes minimum standards for managing intelligence; the APP highlights the importance of grading and reporting intelligence, which is relevant in the context of FRT when deployments are intelligence-led.

[116] *Tele2 Sverige AB v. Post-och telestyrelsen and Secretary of State for the Home Department v. Watson and others, Judgement*, Grand Chamber, Court of Justice of the European Union, cases C-203/15, C-698/15 (21 December 2016) <https://curia.europa.eu/juris/document/document.jsf?text=&docid=186492&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=1088733 > [accessed 14 July 2022], para. 115.

[117] Information Commissioner's Office, *Information Commissioner's Opinion: The Use of Live Facial Recognition Technology in Public Places*, p. 48.

[118] *R (Bridges) v. Chief Constable of South Wales Police, Judgement*, Court of Appeal, para. 130.

[119] Information Commissioner's Office, *Information Commissioner's Opinion: The Use of Live Facial Recognition Technology in Public Places*, p. 48.

[120] Information Commissioner's Office, *Information Commissioner's Opinion: The Use of Live Facial Recognition Technology by Law Enforcement in Public Places*, p. 15.

In Accordance with the Law (Human Rights Act 1998) (continued)

C. Are there clear, objective, and limited criteria concerning third-party access to the data collected or retained, including with regard to what data can be shared, with whom it can be shared, and for what specific purpose it can be shared?

Source: HRA Article 8(2), ECHR Guidance, *Marper* Case, Surveillance Camera Guidance
To be lawful, FRT's interference with Article 8 privacy rights of the Human Rights Act 1998 must be 'in accordance with the law'. In the *S. and Marper v. United Kingdom* court case, the European Court of Human Rights noted that for biometric data processing to be 'in accordance with law', safeguards concerning access of third parties are essential: 'it is as essential, in this context, as in telephone tapping, secret surveillance and covert intelligence-gathering, to have clear, detailed rules governing the scope and application of measures, as well as minimum safeguards concerning, inter alia, duration, storage, usage, access of third parties, procedures for preserving the integrity and confidentiality of data and procedures for its destruction, thus providing sufficient guarantees against the risk of abuse and arbitrariness'.[121] ECHR guidance on Article 8 reiterates the necessity of these safeguards to protect against arbitrary interference.[122] The Surveillance Camera Code of Practice also establishes the principle that: 'Access to retained images and information should be restricted and there must be clearly defined rules on who can gain access and for what purpose such access is granted'.[123]

Necessary in a Democratic Society (Human Rights Act 1998)

D. Have police identified less intrusive alternative measures and proven that FRT is strictly necessary compared to these measures using scientifically verifiable evidence?

Source: HRA Article 8(2), *Bridges Case*, European Data Protection Supervisor
The 'necessary in a democratic society' requirement of Article 8(2) of the Human Rights Act mandates that the legal test of necessity is satisfied. The *Bridges* court case considers the four-part test in *Bank Mellat v. Her Majesty's Treasury (No 2)*, which includes the criteria of 'whether a less intrusive measure could have been used without unacceptably compromising the objective'.[124] The European Data Protection Supervisor notes that based on case law, a key component of the necessity test is providing 'scientifically verifiable evidence that can genuinely support the claim that existing measures and less intrusive alternative measures cannot effectively address the problem'.[125] Additionally, case law 'applies a strict necessity test for any limitations on the exercise of the rights to personal data protection and respect for private life with regard to the processing of personal data'.[126]

[121] *S. and Marper v. United Kingdom, Judgement*, ECtHR 1581, app. nos 30562/04, 30566/04 (4 December 2008) <https://www.bailii.org/eu/cases/ECHR/2008/1581.html> [accessed 14 July 2022], para. 99.

[122] European Court of Human Rights, *Guide on Article 8 of the European Convention on Human Rights – Right to Respect for Private and Family Life, Home and Correspondence* (31 August 2021) <https://www.echr.coe.int/documents/guide_art_8_eng.pdf> [accessed 14 July 2022], para. 623, 638.

[123] Home Office, *Surveillance Camera Code of Practice*, p. 9.

[124] *R (Bridges) v. Chief Constable of South Wales Police*, Judgement, Court of Appeal, para. 132.

[125] European Data Protection Supervisor, *Assessing the Necessity of Measures that Limit the Fundamental Right to the Protection of Personal Data: A Toolkit* (11 April 2017) <https://edps.europa.eu/sites/edp/files/publication/17-06-01_necessity_toolkit_final_en.pdf> [accessed 14 July 2022], p. 18.

[126] European Data Protection Supervisor, *Assessing the Necessity of Measures*, p. 7.

Necessary in a Democratic Society (Human Rights Act 1998) (continued)
E. Have police conducted distinct necessity tests with an evidence-based justification for each category of individuals on the watchlist?
Source: HRA Article 8(2), Essex Report, European Data Protection Supervisor The 'necessary in a democratic society' requirement of Article 8(2) of the Human Rights Act mandates that the legal test of necessity is satisfied. In the context of the Metropolitan Police Service (MPS) use of LFR, the University of Essex report notes that, 'The European Court of Human Rights case law regarding custody images, finger prints, and DNA samples, indicates that there are clear differences between the categories of persons potentially included on the watchlist […] in light of the distinctions between different categories of persons, and on the basis of the longstanding case law, it appears inappropriate that the MPS include all categories of persons within the same necessity analysis: distinct analysis is likely to be required'.[127] Based on case law, the European Data Protection Supervisor also notes that a key component of the necessity test is providing an evidence-based justification.[128]
F. Have police shown that FRT does not disproportionately limit the human rights of affected persons, including those who are misidentified, not on the watchlist, or impacted by unwarranted intrusions?
Source: HRA Article 8(2), *Bridges* Case, Essex Report, European Data Protection Supervisor The 'necessary in a democratic society' requirement of Article 8(2) of the Human Rights Act mandates that the legal test of proportionality is satisfied. In the *Bridges* court case, the High Court accepted that LFR engages with Article 8 or the privacy rights of anyone whose face is scanned by the technology.[129] Thus, it is critical for a proportionality assessment to consider the impact on those not on the watchlist. Guidance from the European Data Protection Supervisor also indicates that a proportionality analysis should assess the impact to the rights of those not on the watchlist. The guidance notes that the assessment should consider the scope of the interference, including the 'number of people affected; whether it raises "collateral intrusions", that is interference with the privacy of persons other than the subjects of the measure'.[130] The University of Essex report reiterates these points, arguing that the Metropolitan Police Service's proportionality analysis 'is inappropriately narrow, and fails to adequately take into account the impact that the deployment of LFR technology has on those individuals who do not appear on the watchlist but who are subject to data processing by the LFR technology, or the impact on those individuals who are incorrectly identified as being on the watchlist (i.e. as a result of false positives)'.[131]

[127] Fussey and Murray, *Independent Report*, p. 58.

[128] European Data Protection Supervisor, *Assessing the Necessity of Measures*, p. 18.

[129] *R (Bridges) v. Chief Constable of South Wales Police*, Judgement, High Court, Queen's Bench Division, case CO/4085/2018 (4 September 2019) <https://www.judiciary.uk/wp-content/uploads/2019/09/bridges-swp-judgment-Final03-09-19-1.pdf> [accessed 14 July 2022], para. 59.

[130] European Data Protection Supervisor, *Guidelines on Assessing the Proportionality of Measures*, p. 23.

[131] Fussey and Murray, *Independent Report*.

Data Protection (Data Protection Act 2018)
G. Before using FRT, have police carried out and published a data protection impact assessment and appropriate policy document for sensitive data processing?
Source: DPA18 Section 35, DPA18 Section 64, ICO Section 64 of the Data Protection Act 2018 requires that the data controller (in this case, the police) carries out a DPIA prior to the data processing for high-risk operations such as FRT. Additionally, Section 35 of the Data Protection Act 2018 requires an appropriate policy document for sensitive data processing. The ICO guidance also reiterates that under data protection law, a DPIA and appropriate policy document are required for police use of FRT.[132]
H. Beyond social media or website publishing, have police used other means to inform potential data subjects or most people in their jurisdiction in advance about when, where, why, and how FRT is being used and how they can exercise their individual rights?
Source: DPA18 Section 44, GDPR Article 5(1)(a) and Articles 13 to 14, ICO Section 44 of the Data Protection Act 2018 imposes duties on police to make information about data processing available to data subjects. The ICO's opinion on the use of LFR in public spaces notes that, 'Transparency is a key component of fairness, as well as being a legal requirement under UK GDPR Articles 5(1)(a), 13 and 14. Controllers must provide clear information to data subjects about when, where and why they are using LFR and how individuals can exercise their data protection rights […] The ICO has seen examples where the quality of information for the public and the locations and visibility of signage have been insufficient […] Controllers should consider more extensive and effective measures to ensure that the public understands how their data is being processed'.[133]
I. Are there clear measures to ensure data subjects can exercise their individual rights including the rights to rectification, erasure, and object with clear justifications if exemptions apply?
Source: DPA18 Sections 45 to 50, GDPR Articles 12 to 22, ICO, Police Force Documents Sections 45 to 50 of the Data Protection Act 2018 establish the rights of data subjects for the processing of personal data for law enforcement purposes. The ICO's opinion on the use of LFR in public spaces notes that controllers deploying LFR must 'ensure that data subjects are able to exercise their rights, as defined in UK GDPR Articles 12 to 22'.[134] These rights include the right to be informed; the rights of access, rectification, and erasure; and the rights to restrict processing and to object. Exemptions to these rights may apply depending on the purpose for processing the data.[135] Examining the data protection impact assessments carried out by police forces, we noticed that FRT often entails processing for both general purposes and law enforcement purposes. Given the potentially broad range of purposes, it is critical that police provide clear justifications if exemptions to these rights apply.

[132] 132. Information Commissioner's Office, *Information Commissioner's Opinion: The Use of Live Facial Recognition Technology by Law Enforcement in Public Places*, p. 2.

[133] 133. Information Commissioner's Office, *Information Commissioner's Opinion: The Use of Live Facial Recognition Technology by Law Enforcement in Public Places*, p. 39.

[134] 134. Information Commissioner's Office, *Information Commissioner's Opinion: The Use of Live Facial Recognition Technology in Public Places*, p. 28.

[135] 135 Information Commissioner's Office, *Guide to Law Enforcement Processing* (1 January 2021) <https://ico.org.uk/media/for-organisations/guide-to-data-protection/guide-to-le-processing-1-1.pdf> [accessed 14 July 2022], p. 19.

Data Protection (Data Protection Act 2018) (continued)

J. Do police check the watchlist against the data source close to the time of deployment to ensure the watchlist is accurate and up to date?

Source: DPA18 Section 38, GDPR Article 5(1)(d), ICO, Surveillance Camera Guidance
The accuracy data protection principle, established in Article 5(1)(d) of the GDPR and Section 38 of the Data Protection Act 2018, requires that every reasonable step must be taken to ensure that data is accurate and kept up to date. The ICO reiterates this principle in the context of FRT, noting that images on watchlists must be accurate and kept up to date. The Surveillance Camera Code of Practice also establishes the principle that: 'Any information used to support a surveillance camera system which compares against a reference database for matching purposes should be accurate and kept up to date.[136]

K. Are there clear measures to ensure that watchlist images are lawfully held, have a known provenance, and exclude unconvicted custody images?

Source: Civil Society on FRT, College of Policing, ICO, *RMC* Case, Scottish Parliament
(a) Lawfully held images: The ICO opinion on law enforcement use of LFR in public spaces notes that watchlists are expected to only include images that are lawfully held by police at the time of use. The ICO opinion on the use of LFR in public spaces also notes controllers are expected to understand the origin of watchlist images as images of uncertain provenance (such as images sourced from social media) will raise issues of lawfulness, fairness, and accuracy. Civil society organisations also raised the concern that the College of Policing's guidance on LFR 'does not limit the watchlist to photos obtained lawfully by the police, and allows police forces to use photos obtained from social media or third parties'.[137] The College of Policing's revised guidance now recommends that watchlists only contain images lawfully held by police.

(b) Exclusion of unconvicted custody images: 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*, that the indefinite retention of custody images of innocent people who are arrested but unconvicted is unlawful. The Scottish Parliament recommended that this issue should be addressed for Police Scotland's use of retrospective facial recognition and that Police Scotland should 'provide details of its plans, including the timescale, for deleting images of innocent people retained on legacy databases'.[138] Civil society organisations such as Big Brother Watch and Open Rights Group have also noted this issue and called for the deletion of innocent people from police databases.[139]

[136] Home Office, *Surveillance Camera Code of Practice*, p. 9.

[137] Privacy International and others, 'Consultation on Live Facial Recognition APP. Feedback Form', p. 9.

[138] Scottish Parliament, Justice Sub-Committee on Policing, *Facial Recognition: How Policing in Scotland Makes Use of This Technology*, p. 45.

[139] Big Brother Watch, *Briefing on Facial Recognition Surveillance*, p. 5; Big Brother Watch and Open Rights Group, 'Joint Submission to the Scottish Parliament Justice Sub-Committee on Policing Inquiry into Facial Recognition: How Policing in Scotland Makes Use of this Technology' (November 2019) <https://bigbrotherwatch.org.uk/wp-content/uploads/2019/11/Big-Brother-Watch-and-Open-Rights-Group-Joint-Submission-to-the-Scottish-Justice-Sub-Committee-on-Policing-inquiry-into-Facial-Recognition-November-2019.pdf> [accessed 14 July 2022], p. 7.

Data Protection (Data Protection Act 2018) (continued)

L. Via direct consultation, have police proactively considered views of the public, especially marginalised communities, on the particular type of FRT and justified a disregard of the views if relevant?

Source: GDPR Article 35(9), ICO
GDPR Article 35(9) mandates that, where appropriate, the controller 'shall seek the views of data subjects or their representatives'.[140] In the context of this requirement, the ICO's opinion on the use of LFR in public spaces notes that, 'it is likely to be appropriate to carry out some form of general public consultation or targeted research. For example, this could involve market research with affected groups […] Any consultation should be an objective process and controllers should be clear about the nature, scope, context, risks and impact of the processing […] If a controller decides to deploy LFR despite clear evidence of public objections, whether raised as part of the controller's consultation or wider public discussion, the DPIA should be clear about the reasons for disregarding the views of individuals'.[141] The ICO also highlights the importance of considering marginalised communities, 'As FRT develops, there is a strong case for further engagement and consultation, with particular attention to the concerns of minority ethnic groups'.[142]

M. Have police published their procurement contracts and data-sharing agreements with other parties?

Source: Civil Society on Technology, ICO
The ICO guidance raises the concern of sharing watchlists between law enforcement and private sector organisations and notes that having a data-sharing agreement is good practice. Big Brother Watch also calls for 'a public inventory of public-private information sharing agreements […] to improve transparency and allow for harmful information sharing agreements to be challenged'.[143]

Non-Discrimination (Human Rights Act 1998 and Equality Act 2010)

N. Before using FRT, have police carried out and published an equality impact assessment?

Source: PSED, Civil Society on FRT, ICO
While the Public Sector Equality Duty (PSED) of the Equality Act 2010 does not mandate the undertaking of an Equality Impact Assessment (EIA), the completion and publication of an EIA enables the public to understand and scrutinise how police comply with the PSED. The Information Commissioner has also noted that law enforcement agencies should complete an EIA.[144] WebRoots Democracy also recommends that an EIA should be mandatory prior to any facial recognition deployment.[145]

[140] Information Commissioner's Office, *Information Commissioner's Opinion: The Use of Live Facial Recognition Technology in Public Places*, p. 59.

[141] Information Commissioner's Office, *Information Commissioner's Opinion: The Use of Live Facial Recognition Technology in Public Places*, pp. 59–60.

[142] Information Commissioner's Office, *Information Commissioner's Opinion: The Use of Live Facial Recognition Technology in Public Places*, p. 25.

[143] Big Brother Watch, 'Written Evidence for the Justice and Home Affairs Committee's Inquiry into New Technologies and the Application of the Law' (September 2021) <https://bigbrotherwatch.org.uk/wp-content/uploads/2022/05/Final-Big-Brother-Watch-Briefing-to-JHAC-on-new-technologies-and-the-application-of-the-law-Final10476.pdf> [accessed 14 July 2022], p. 32.

[144] Information Commissioner's Office, *Information Commissioner's Opinion: The Use of Live Facial Recognition Technology by Law Enforcement in Public Places*, p. 19.

[145] Areeq Chowdhury, *Unmasking Facial Recognition: An Exploration of the Racial Bias Implications of Facial Recognition Surveillance in the United Kingdom* (London: WebRoots Democracy, 2020) <https://webrootsdemocracy.files.wordpress.com/2020/08/unmasking-facial-recognition-webroots-democracy.pdf> [accessed 14 July 2022], p. 37.

Non-Discrimination (Human Rights Act 1998 and Equality Act 2010) (continued)

O. For each deployment, have police published the demographic makeup of the watchlist?

Source: HRA Article 14, PSED, Civil Society on Technology, ICO, Police Force Documents
Fairness and non-discrimination are codified in Article 14 of the Human Rights Act 1998, Public Sector Equality Duty, and GDPR Article 5(1)(a). The ICO opinion notes that, 'there is a risk of bias and discrimination in the process of compiling watchlists [...] these processes risk reinforcing existing biases in society'.[146]
In their DPIA on their use of LFR, South Wales Police addresses the risk of 'a disproportionate number of individuals with protected characteristics being identified in False Alerts' by noting that 'Watchlists will also be checked to ensure that gender or ethnicity is not unfairly represented'.[147] To improve accountability to the public, the demographic breakdown of the watchlist should be available for public scrutiny in order to assess whether certain groups are unfairly represented. Civil society organisations have also highlighted the disproportionate composition of Black people in police databases such as the Metropolitan Police Service's Gangs Violence Matrix.[148]

P. For each deployment, have police published the demographic makeup of the population where FRT is used?

Source: HRA Article 14, PSED, Civil Society on FRT, ICO
Fairness and non-discrimination are codified in Article 14 of the Human Rights Act 1998, Public Sector Equality Duty, and GDPR Article 5(1)(a). The ICO opinion on the use of LFR notes that the Information Commissioner expects controllers using LFR to 'monitor the outcomes of the system, including for any evidence of bias or discrimination'.[149] WebRoots Democracy recommends that ethnicity data is collected and reported, as 'understanding how the technology impacts different demographics will be essential in determining whether or not its use is fair and proportionate'; the report highlights the importance of having 'data on who has been targeted, who has been flagged, and who has been arrested'.[150] Civil society organisations such as Liberty and Big Brother Watch have also raised concerns about the discriminatory use of FRT on people of colour.[151]

Q. For each deployment, have police published the demographic data for arrests, stop and searches, and other outcomes resulting from the use of FRT?

Source: HRA Article 14, PSED, Civil Society on FRT, ICO
Fairness and non-discrimination are codified in Article 14 of the Human Rights Act 1998, Public Sector Equality Duty, and GDPR Article 5(1)(a). The ICO highlights the importance of monitoring outcomes of FRT for any evidence of discrimination.[152] WebRoots Democracy also recommends that ethnicity data, including who has been arrested, is reported in order to assess fairness and proportionality.[153] Civil society organisations have also raised concerns about FRT's disproportionate misidentifications of women and people of colour and the resulting unwarranted intrusions such as stop and search.[154]

[146] Information Commissioner's Office, *Information Commissioner's Opinion: The Use of Live Facial Recognition Technology in Public Places*, pp. 21, 39.

[147] South Wales Police, 'Data Protection Impact Assessment for Live Facial Recognition (LFR)' <https://www.south-wales.police.uk/SysSiteAssets/media/downloads/south-wales/about-us/live-facial-recognition/lfr-dpia-v0.4.pdf> [accessed 17 July 2022], pp. 34, 37.

[148] Amnesty International, *Trapped in the Matrix*, p. 15.

[149] Information Commissioner's Office, *Information Commissioner's Opinion: The Use of Live Facial Recognition Technology in Public Places*, p. 39.

[150] Chowdhury, *Unmasking Facial Recognition*, p. 37.

[151] Liberty, 'Briefing on the Amended Surveillance Camera Code of Practice', pp. 5–6; Big Brother Watch, *Briefing on Facial Recognition Surveillance*, pp. 23–24.

[152] Information Commissioner's Office, *Information Commissioner's Opinion: The Use of Live Facial Recognition Technology in Public Places*, p. 39.

[153] Chowdhury, *Unmasking Facial Recognition*, p. 37.

[154] Liberty, 'Briefing on the Amended Surveillance Camera Code of Practice', pp. 5–6; Big Brother Watch, *Briefing on Facial Recognition Surveillance*, pp. 23–24.

Free Expression and Assembly (Human Rights Act 1998)

R. Have police assessed FRT's potential 'chilling effect' on the rights to freedom of expression and assembly to inform the legal test of 'necessary in a democratic society'?

Source: HRA Articles 10 and 11, ECHR Guidance
In order to assess whether FRT's interference with Article 8 privacy rights is 'necessary in a democratic society', it is essential to identify the full range of rights impacted. This includes FRT's impact on the rights to freedom of expression and assembly, protected by Articles 10 and 11 of the Human Rights Act 1998. ECHR's guidance highlights the importance of considering a chilling effect when assessing whether there has been an interference with the rights to freedom of expression and assembly.[155]

S. Do police preclude using FRT to identify those peacefully participating in an assembly?

Source: HRA Article 11, UN Human Rights
The UN High Commissioner for Human Rights recommended that States '[n]ever use facial recognition technology to identify those peacefully participating in an assembly' in a report examining the impact of new technologies on human rights in the context of assemblies; the High Commissioner notes that: 'The negative effects of the use of facial recognition technology on the right of peaceful assembly can be far-reaching, as United Nations human rights experts have pointed out. Many people feel discouraged from demonstrating in public places and freely expressing their views when they fear that they could be identified and suffer negative consequences'.[156]

[155] European Court of Human Rights, *Guide on Article 10 of the European Convention on Human Rights – Freedom of Expression* (30 April 2021) <https://www.echr.coe.int/documents/guide_art_10_eng.pdf> [accessed 14 July 2022], para. 52; European Court of Human Rights, *Guide on Article 11 of the European Convention on Human Rights – Freedom of Assembly and Association* (30 April 2022) <https://www.echr.coe.int/Documents/Guide_Art_11_ENG.pdf> [accessed 14 July 2022], para. 77.

[156] United Nations High Commissioner for Human Rights, *Impact of New Technologies on the Promotion and Protection of Human Rights in the Context of Assemblies, Including Peaceful Protests - Report.*

C.2 Technical reliability

Algorithmic Fairness (Equality Act 2010)

A. Before using FRT, have police evaluated and published the demographic makeup of the training dataset to ensure the dataset is representative of the population where it is to be used?

Source: PSED, *Bridges* Case, Civil Society on FRT
In the *Bridges* case, the Court of Appeal established that the Public Sector Equality Duty (PSED) of the Equality Act 2010 requires police forces to take all reasonable steps themselves to ensure that the facial recognition software does not have a racial or gender bias. Discussions in the court case highlighted the importance of evaluating the demographic composition of the FRT algorithm training dataset, given that FRT algorithms have been shown to have bias. Civil society organisations have also highlighted the inherent bias in FRT algorithms and the importance of understanding such bias. For example, in a response to the College of Policing's guidance on LFR, civil society organisations responded that, 'the guidance should discourage forces from procuring software where there are constraints on analysing the underlying data, or at least make explicit that commercial secrecy cannot be relied on for any failure to understand inbuilt bias'.[157] Finally, in addition to the PSED, Article 14 of the Human Rights Act 1998 also prohibits discrimination in the UK.

B. Before using FRT, have police evaluated and published FRT's performance across demographic groups, in different conditions that match FRT's operational use, to ensure FRT performs well and similarly across the population?

Source: PSED, *Bridges* Case, NIST, Police Force Documents
In the *Bridges* case, the Court of Appeal established that the Public Sector Equality Duty (PSED) of the Equality Act 2010 requires police forces to take all reasonable steps themselves to ensure that the facial recognition software does not have a racial or gender bias. We examined the equality impact assessments conducted by police forces as well as evaluations conducted by the National Institute of Standards and Technology (NIST). We noticed that the evaluation results vary significantly based on how facial recognition was tested. For example, evaluating facial recognition on high-quality images produced better results than evaluating facial recognition on low-quality images. Thus, we assess if police conduct an evaluation of FRT based on how the technology is used operationally.

[157] Privacy International and others, 'Consultation on Live Facial Recognition APP', p. 9.

Robust Practice (Data Protection Act 2018)

C. Are there safeguards precluding the use of FRT with an unsuitable low-quality probe or watchlist image?

Source: DPA18 Section 38, GDPR Article 5(1)(d), Cardiff Report, ICO
The accuracy data protection principle, established in Article 5(1)(d) of the GDPR and Section 38 of the Data Protection Act 2018, requires that every reasonable step must be taken to ensure that data is accurate and kept up to date. The ICO opinion on the use of LFR in public spaces discusses the issue of accuracy and notes that too many incorrect matches 'will call into question both the fairness and the necessity of the processing'.[158] The Cardiff University's evaluation of South Wales Police's facial recognition trial also noted that the quality of probe images was important for the performance of police officers reviewing the FRT matches.[159] In this audit question, we assess if there are safeguards to prevent the use of FRT with a low-quality image that is likely to produce an incorrect match.

D. Have police pre-established and met thresholds for the FRT system's accuracy (precision, false positive rate, true positive rate) to inform the legal test of strict necessity for personal data processing?

Source: DPA18 Section 35, *Bridges* Case, ICO
DPA 18 Section 35(5) mandates strict necessity for personal data processing. The ICO opinion on the use of LFR in public spaces notes the importance of measuring the LFR system's accuracy: 'The law does not stipulate a specific threshold for precision or recall. This is for the controller to establish to ensure their processing is necessary, proportionate and compliant. It is good practice to establish these thresholds in the DPIA. In the Bridges case, the ability of the police force's LFR system to accurately identify persons of interest was a factor in the Divisional Court's finding that any interference with the claimant's ECHR Article 8 rights was proportionate in those circumstances'.[160]

Deployment Performance (Equality Act 2010)

E. Does FRT perform well (precision, false positive rate, true positive rate) and similarly across demographic groups?

Source: PSED, ICO
In the *Bridges* case, the Court of Appeal established that the Public Sector Equality Duty (PSED) of the Equality Act 2010 requires police forces to take all reasonable steps themselves to ensure that the facial recognition software does not have a racial or gender bias. To comply with the PSED, it is crucial that police forces assess the FRT deployment performance across demographic groups. The ICO opinion on the use of LFR in public spaces also notes that controllers using FRT should 'monitor the outcomes of the system, including for any evidence of bias or discrimination' in order to comply with the fairness and transparency principles established in Article 5(1)(a) of the UK GDPR.[161]

[158] Information Commissioner's Office, *Information Commissioner's Opinion: The Use of Live Facial Recognition Technology in Public Places*, p. 38.

[159] Davies, Innes, and Dawson, *An Evaluation of South Wales Police's Use of Automated Facial Recognition*, p. 35.

[160] Information Commissioner's Office, *Information Commissioner's Opinion: The Use of Live Facial Recognition Technology in Public Places*, p. 65.

[161] Information Commissioner's Office, *Information Commissioner's Opinion: The Use of Live Facial Recognition Technology in Public Places*, p. 39.

C.3 Human decision-making

Human Review

A. Is there a transparent evaluation that shows human review of the FRT matches is reliable, given the accuracy of officer-verified matches and the amount of time an officer has to review an FRT match?

Source: Essex Report, House of Lords, Surveillance Camera Guidance
The House of Lords report highlights the importance of a 'human in the loop' or meaningful human engagement in any process that uses technology in its decision-making.[162] The Surveillance Camera Code of Practice also notes that the use of FRT 'should always involve human intervention before decisions are taken that affect an individual adversely'.[163] In this context, the former Surveillance Camera Commissioner recommends that 'senior officers should ask themselves how they select, train, instruct, deploy, manage and analyse the performance of the human decision maker'.[164] Thus, it is critical to assess the human review of FRT, especially given that this review has been found to be unreliable. For example, the University of Essex report on the Metropolitan Police Service's use of LFR notes that officers had little time to review FRT matches (due to the live nature of the FRT deployment) and that the accuracy of officer-verified matches was low.[165] In this question, we assess the quality of the human review of FRT matches based on the accuracy of officer-verified matches and the amount of time officers have for reviewing FRT matches. For effective review, it is critical that there is sufficient delay between the point at which an FRT match is generated, and the point at which an officer makes a decision.

Preparation

B. Is training for the particular type of FRT mandated for police officers using the technology?

Source: House of Lords
The House of Lords report notes that for new technologies including facial recognition, 'There are no legal requirements for users to be trained, nor any standards available for what available training should include'.[166] The report calls for 'mandatory training for officers and officials using advanced technologies' and notes that this training should include 'both generic data analytics and specificities of the particular technology in question'.[167]

C. Are there clear standards for technical training on using FRT, data protection training, and training on risks including differential treatment, function creep, and unwarranted intrusions?

Source: House of Lords
The House of Lords report highlights the current lack of training standards and notes that 'there should be mandatory training for officers and officials on the use of the tools themselves as well as general training on the legislative context, the possibility of bias and the need for cautious interpretation of the outputs'.[168] Here, we assess if there are training standards for the use of FRT with regard to the relevant legislative context (data protection) and the possibility of bias and harm (including differential treatment and unwarranted intrusions).

[162] House of Lords, Justice and Home Affairs Committee, *Technology Rules?*, p. 47.

[163] Home Office, *Surveillance Camera Code of Practice*, p. 11.

[164] Porter, *Facing the Camera*, p. 50.

[165] Fussey and Murray, *Independent Report*, pp. 74, 120.

[166] House of Lords, Justice and Home Affairs Committee, *Technology Rules?*, p. 52.

[167] House of Lords, Justice and Home Affairs Committee, *Technology Rules?*, p. 54.

[168] House of Lords, Justice and Home Affairs Committee, *Technology Rules?*, p. 5.

Preparation (continued)

D. Has there been a documented non-operational research trial of FRT with informed consent from participants before the operational use of FRT for policing?

Source: BFEG, Essex Report, London Policing Ethics Panel
Several bodies including the London Policing Ethics Panel and the Biometrics and Forensics Ethics Group have highlighted the ethical concerns that arise when facial recognition trials are also policing operations.[169] The University of Essex report on the Metropolitan Police Service's use of LFR discusses how combining trials with operational deployments raises issues of consent and public trust.[170] For example, ensuring consent for participation in the trial can conflict with policing purposes.

Accountability

E. Are there clear measures for police to document cases of harm resulting from the use of FRT such as differential treatment, function creep, or unwarranted intrusions?

Source: House of Lords
Transparency about the harms of police use of FRT is critical for public scrutiny. The House of Lords report highlights the importance and current lack of transparency with regard to how new technologies are currently being used by law enforcement. The report notes the importance of establishing requirements when there is harm: 'It was suggested that an initial step to achieving greater transparency would be a public administration "duty of candour". As it stands, there is no statutory duty of candour on the police. Duty of candour obligations apply largely in health care settings and the relevant legislation sets out some specific requirements to be followed when things go wrong; including informing people about the incident, providing reasonable support, providing truthful information, and an apology'.[171]

F. Do police have a whistleblower protection policy to protect persons who reveal FRT misuse?

Source: Civil Society on Technology, Local Oversight
Many civil society groups have illustrated how UK police forces have secretly used technology that can be used in discriminatory ways.[172] The secret use of technology by police raises the importance of establishing a whistleblower protection police in order to protect whistleblowers who reveal wrongdoings. The proposed Surveillance Oversight ordinance, which was developed by the TRUST San Diego Coalition and will be put to vote by the San Diego City Council, highlights the issue of secrecy of surveillance technology; the ordinance mandates whistleblower protections as well as the public disclosure of the City's surveillance-related contracts.[173]

[169] London Policing Ethics Panel, 'Interim Report on Live Facial Recognition', p. 9; London Policing Ethics Panel, 'Final Report on Live Facial Recognition', p. 31; Nina Hallowell, Louise Amoore, Simon Caney, and Peter Waggett, *Ethical Issues Arising from the Police Use of Live Facial Recognition Technology: Interim Report of the Biometrics and Forensics Ethics Group Facial Recognition Working Group* (February 2019) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/781745/Facial_Recognition_Briefing_BFEG_February_2019.pdf> [accessed 14 July 2022], p. 3.

[170] Fussey and Murray, *Independent Report*, pp. 23–26.

[171] House of Lords, Justice and Home Affairs Committee, *Technology Rules?*, p. 41.

[172] Amnesty International, *Trapped in the Matrix*; Big Brother Watch, *Briefing on Facial Recognition Surveillance*; Privacy International, 'Digital Stop and Search: How the UK Police Can Secretly Download Everything from Your Mobile Phone' (March 2018) <https://privacyinternational.org/sites/default/files/2018-03/Digital%2520Stop%2520and%2520Search%2520Report.pdf> [accessed 14 July 2022].

[173] TRUST San Diego Coalition, 'City of San Diego, Proposed Surveillance Ordinance and Privacy Commission' <https://sandiegotrust.org/City_of_San_Diego_Proposed_Surveillance_Ordinance_and_Privacy_Commission.pdf> [accessed 14 July 2022], p. 12.

Accountability (continued)

G. Is there a clear redress mechanism (beyond judicial review and usual complaint procedures) for harmed individuals and groups to participate in an investigation into police use of FRT?

Source: Civil Society on Technology, House of Lords
The House of Lords Justice and Home Affairs Committee highlighted the lack of recourse mechanisms for people harmed by the use of new technologies in law enforcement. The Committee concluded that judicial reviews and the usual complaint procedures are insufficient mechanisms for accountability. Courts can only conduct judicial reviews 'if a case or challenge is brought to them, with all the requirements on individuals and resources that that entails. The role of courts in society is of course vital, but they are not a substitute for robust accountability mechanisms'.[174] The Committee also found that the current 'complaints mechanisms play a limited role in holding law enforcement to account in their use of advanced technologies'.[175] Numerous civil society groups have also called for provisions for individual and collective redress in the forthcoming EU Artificial Intelligence Act.[176]

H. Are there clear measures to ensure that the redress mechanism is procedurally fair?

Source: HRA Article 6
Procedural justice in the context of a trial is guaranteed by HRA Article 6, the right to a fair trial. Procedural justice refers to the fairness of a procedure by which a decision is made and is critical to ensure a fair trial as well as a fair redress mechanism. Here, we assess if there are clear measures to ensure that the redress mechanism for those harmed by FRT is procedurally fair.

[174] House of Lords, Justice and Home Affairs Committee, *Technology Rules?*, p. 37.

[175] House of Lords, Justice and Home Affairs Committee, *Technology Rules?,* p. 37.

[176] European Digital Rights, Access Now, Panoptykon Foundation, epicenter.works, AlgorithmWatch, European Disability Forum, Bits of Freedom, Fair Trials, PICUM, and ANEC (European Consumer Voice in Standardisation), *An EU Artificial Intelligence Act for Fundamental Rights: A Civil Society Statement* (30 November 2021) <https://edri.org/wp-content/uploads/2021/12/Political-statement-on-AI-Act.pdf> [accessed 14 July], pp. 4–5.

C.4 Expertise and oversight

Ethics Committee
A. Is regular oversight from an ethics committee mandated throughout the life of the FRT project?
Source: BFEG, House of Lords The House of Lords report highlights the importance of continuing oversight: 'Oversight mechanisms are required to complement pre-deployment scientific evaluations of new technologies used for the application of the law. Local specialist ethics committees are best placed to scrutinise technological solutions throughout their lifecycle and in their deployment contexts'.[177] The Biometrics and Forensics Ethics Group (BFEG) also recommends regular oversight from an ethics body: 'The BFEG suggests that an independent ethics group should be tasked to oversee a) individual deployments of biometric recognition technologies by the police and b) the use of biometric recognition technologies in [public-private collaborations]. This independent ethics group would require that any proposed deployments and [public-private collaborations] are reviewed when they are established and monitored at regular intervals during their operation'.[178]
B. Are there clear processes for the committee to influence if and how FRT is implemented, including the power of veto for the FRT project?
Source: House of Lords, Local Oversight The House of Lords report cites academics who 'stressed the importance of a clear statutory basis, budget, and power for ethics committees to have the "capacity to scrutinise and hold technology developers, users and commissioners to account."'[179] The San Diego Privacy Advisory Board, which might serve as a model for a committee overseeing the use of FRT, reviews any proposed use of surveillance technology and 'may make a recommendation to the City Council by voting its approval to proceed, object to the proposal, recommend that the City staff modify the proposal, or take no action'.[180] In this question, we assess if the ethics committee holds the power to influence and veto the use of FRT, which is crucial in order for the committee to provide meaningful scrutiny.
C. Is the committee an independent body from police organisations with members having non-policing backgrounds and with safeguards to ensure the committee's sustainability even without political support?
Source: BFEG, Civil Society on FRT, House of Lords, Surveillance Camera Guidance The House of Lords report discusses the importance of oversight from ethics committees that are independent: 'These committees should be granted independence, a statutory basis, and an independent budget'.[181] The former Surveillance Camera Commissioner recommends that 'where police forces are considering operating LFR they should develop mechanisms which provide for meaningful and independent "ethical oversight" of their decision making and operational conduct'.[182] Privacy International and the Biometrics and Forensics Ethics Group also note the importance of independent oversight and scrutiny.[183]

[177] House of Lords, Justice and Home Affairs Committee, *Technology Rules?*, p. 75.

[178] Biometrics and Forensics Ethics Group, *Briefing Note*, p. 9.

[179] House of Lords, Justice and Home Affairs Committee, *Technology Rules?*, p. 75.

[180] TRUST San Diego Coalition, 'City of San Diego, Proposed Surveillance Ordinance and Privacy Commission', p. 8.

[181] House of Lords, Justice and Home Affairs Committee, *Technology Rules?*, p. 75.

[182] Porter, *Facing the Camera*, p. 19.

[183] Privacy International, 'Submission to the Scottish Parliament's Justice Sub-Committee on Policing's Inquiry into Facial Recognition Policing' (November 2019) <https://privacyinternational.org/sites/default/files/2020-04/19.11.01_JusticeSC_FRT_Evidence_PI_FINAL_2%20%282%29.pdf> [accessed 14 July 2022], p. 13; Biometrics and Forensics Ethics Group, *Briefing Note*, p. 9.

Ethics Committee (continued)
D. Is the committee diverse in terms of demographic makeup and independent expertise in human rights, equality, and data protection?
Source: Civil Society on FRT, House of Lords, Local Oversight The House of Lords report highlights the importance of diverse membership and independence for ethics committees overseeing police use of new technologies.[184] Expertise in human rights, equality, and data protection is especially important given FRT's impact on these rights. Privacy International also recommends that FRT is not used under any circumstance unless an 'independent review and scrutiny takes place as to whether the use of FRT […] does or could meet human rights and data protection safeguards including data minimisation and data protection by design'.[185] Additionally, the West Midlands Ethics Committee and the San Diego Privacy Advisory Board, which might serve as models for a committee overseeing the use of FRT, highlight the importance of diversity in terms of demographic makeup and expertise in human rights, equality, and data protection: (1) The West Midlands Ethics Committee oversees data science projects proposed by West Midlands Police. The committee's Terms of Reference note that the committee will typically include members with expertise in human rights and knowledge of data protection rights and issues concerned with bias and discrimination; the Terms of Reference also state that all reasonable endeavours will be used 'to appoint Ethics Committee members that are, so far as is possible, representative of the diverse communities of the West Midlands including in relation to age, race, colour, nationality, religion, belief, sex, gender, pregnancy & maternity, disability, sexual orientation or otherwise'.[186] (2) The San Diego Privacy Advisory Board also notes that there must be members representing 'equity-focused organizations serving or protecting the rights of communities and groups historically subject to disproportionate surveillance, including diverse communities of colour, immigrant communities, religious minorities, and groups concerned with privacy and protest'.[187]
E. Are detailed meeting minutes published, including briefing papers, discussions, and conclusions?
Source: House of Lords, Local Oversight The House of Lords report highlights the importance of a committee's commitment to transparency.[188] The West Midlands Ethics Committee, which might serve as a model for an oversight committee, publishes detailed meeting minutes, including briefing papers, discussions, and conclusions.[189]

[184] House of Lords, Justice and Home Affairs Committee, *Technology Rules?*, p. 75.

[185] Privacy International, 'Submission to the Scottish Parliament's Justice Sub-Committee on Policing's Inquiry into Facial Recognition Policing', p. 13.

[186] West Midlands Police and Crime Commissioner, 'West Midlands Police's Ethics Committee: Terms of Reference'.

[187] TRUST San Diego Coalition, 'City of San Diego, Proposed Surveillance Ordinance and Privacy Commission', p. 18.

[188] House of Lords, Justice and Home Affairs Committee, *Technology Rules?*, pp. 74–75.

[189] West Midlands Police and Crime Commissioner, 'West Midlands Police's Ethics Committee: Terms of Reference'.

Civil Society and Experts

F. Are there transparent, proactive consultations with civil society and independent experts on the particular type of FRT?

Source: Civil Society on FRT, Essex Report, House of Lords
The House of Lords report highlights that: ‘Several witnesses recommended that “assessments should be published and consultation should be enabled in a real and transparent sense with both the public and civil society prior to deployment”’.[190] For consultations with civil society and experts to be meaningful, it is essential that they are transparent, proactive, and focused on the specific use of FRT. Privacy International also recommends that FRT is not used under any circumstance unless a ‘transparent, informed and detailed consultation has taken place engaging both the public and civil society’.[191] The University of Essex report on the Metropolitan Police Service use of live FRT also highlights the concern of reactive rather than proactive consultations with civil society.[192]

G. Are police required to consider the advice from consultations and transparently explain the outcomes, including providing a justification if the advice is not followed?

Source: Essex Report, UK Cabinet Office
The UK Cabinet Office’s consultation principles highlight the importance of explaining how consultation responses have informed the policy being considered in order to facilitate scrutiny.[193] In the context of police use of FRT, if police do not follow the advice from consultations, they should explain the reason for doing so. The University of Essex report on the Metropolitan Police Service (MPS) use of live FRT also highlights that although MPS established a ‘stakeholder group’ with public opponents of live FRT including civil society groups, the effectiveness of the stakeholder group was unclear.[194] In this question, we assess the effectiveness of consultations, by evaluating whether police are required to consider the advice from consultations and whether the outcomes are documented and published.

[190] House of Lords, Justice and Home Affairs Committee, *Technology Rules?*, p. 60.

[191] Privacy International, ‘Submission to the Scottish Parliament’s Justice Sub-Committee on Policing’s Inquiry into Facial Recognition Policing’, p. 13.

[192] Fussey and Murray, *Independent Report*, p. 63.

[193] Cabinet Office, ‘Consultation Principles: Guidance’, *Gov.uk* (19 March 2018) <https://www.gov.uk/government/publications/consultation-principles-guidance> [accessed 14 July 2022]

[194] Fussey and Murray, *Independent Report*, p. 63.

Community Engagement

H. Are there clear, proactive processes for the public, especially marginalised communities, to influence if and how FRT is implemented?

Source: Civil Society on Technology, House of Lords, UK Cabinet Office
In the context of community consultations, the House of Lords report highlights points raised by witnesses about the importance of (a) involving affected communities in the policy decisions about implementing new technologies and (b) involving communities from an early stage 'in the deployment and evaluation of technological solutions, so they can flag potential risks that technology providers and customers may have overlooked'.[195] Additionally, as part of their Tech Equity Coalition, the ACLU has highlighted the need to 'uplift the voices of historically marginalized communities in decisions about technology'.[196] The ACLU's Community Control Over Police Surveillance Model Bill also notes that this is crucial for surveillance technologies, given that 'surveillance efforts have been used to intimidate and oppress certain communities and groups more than others'.[197] The UK Cabinet Office's consultation principles also note the importance of clarifying how consultation responses have informed the policy being considered.[198] Here, we assess if there are clear, proactive processes for the public, especially marginalised communities, to influence the implementation of facial recognition.

I. Are all FRT materials accessible to people with disabilities and provided in immigrant languages?

Source: PSED, Civil Society on Technology
The Public Sector Equality Duty of the Equality Act 2010 requires that police forces have due regard to meet the needs of people with disabilities. The Public Sector Bodies (Websites and Mobile Applications) (No. 2) Accessibility Regulations 2018 establish additional obligations to make police force websites accessible to people with disabilities. Additionally, for the forthcoming EU Artificial Intelligence Act, numerous civil society organisations have called for: 'The inclusion of horizontal and mainstreamed accessibility requirements for AI systems irrespective of level of risk, including for AI-related information and instruction manuals, consistent with the European Accessibility Act'.[199] Here, we assess whether FRT materials are made accessible in order to reduce barriers for people with disabilities and immigrants who have fluency in languages other than English.

[195] House of Lords, Justice and Home Affairs Committee, *Technology Rules?*, p. 61.

[196] American Civil Liberties Union, 'Tech Equity Coalition'.

[197] American Civil Liberties Union, 'Community Control Over Police Surveillance (CCOPS) Model Bill'.

[198] Cabinet Office, 'Consultation Principles: Guidance'.

[199] European Digital Rights and others, *An EU Artificial Intelligence Act for Fundamental Rights: A Civil Society Statement*, p. 5.

D. *Bridges* Case on South Wales Police's Trial of Live Facial Recognition

Police Force: South Wales Police (SWP)

Facial Recognition Type: Live Facial Recognition (LFR) or Live Automated Facial Recognition (AFR)

LFR Deployment Dates: Trial deployments from May 2017 to April 2019

Audit Evaluation Date: July 2022

Key Resources Used: *Bridges* Case, **SWP Documents**, **Deployment Results**, **Cardiff University Report**

Our first case study is of the operational trial deployments of live facial recognition (LFR) conducted by South Wales Police (SWP) from May 2017 to April 2019.[200] In *R (Bridges) v. Chief Constable of South Wales Police*, the Court of Appeal ruled that these deployments were unlawful as 'there was no clear guidance on where [LFR] could be used and who could be put on a watchlist, a data protection impact assessment was deficient and the force did not take reasonable steps to find out if the software had a racial or gender bias'.[201] We highlight additional legal and ethical concerns beyond the scope of the court case, including the technology's use at protests and the absence of effective oversight.

SWP did not establish limits on the use of LFR at assemblies. In fact, the technology was used at a peaceful anti-arms protest, interfering with the human rights to freedom of expression and assembly, without evidence that the legal requirements of necessity and proportionality were met.[202] SWP's data protection impact assessment and policy documents did not acknowledge nor address LFR's impact on the rights to freedom of expression and assembly.

There was a lack of effective oversight over the use of LFR. While SWP had early engagements with the SWP Joint Independent Ethics Committee, regular and transparent oversight was not provided throughout the lifecycle of the LFR project.[203] During committee meetings, there were no independent experts in human rights, equality, or data protection in attendance, even though such expertise has been documented as crucial for the oversight of technologies such as LFR.

Moreover, there remained concerns about the committee's independence. Although there were some independent members, the committee also included police officers and is a body situated within the police force. In fact, during meetings, 63% of attendees were members of SWP and 71% were members of either SWP or the South Wales Police and Crime Commissioner. Finally, there were no consultations with the public, especially marginalised communities, on how and whether LFR was implemented.

[200] At the time of the deployments, South Wales Police called the technology live automated facial recognition (AFR) or AFR Locate.

[201] Rees, 'Facial Recognition Use'.

[202] Apple, 'South Wales Police Under Fire'; Big Brother Watch, *Face Off*.

[203] The committee's published meeting minutes indicate that there was only one meeting where LFR was discussed, yet this discussion itself is not published.

Below we provide the full audit scorecard for this case study, which includes the score and accompanying explanation for each question.

D.1 Legal standards

In Accordance with the Law (Human Rights Act 1998)	Score
A. Are there clear, objective, and limited criteria for who can be included in the watchlist, including with regard to the image source and the seriousness of offence or risk?	0 / 1
Notes: The watchlist criteria was not clear, objective, or limited. In the *Bridges* case, the Court of Appeal noted that, 'It is not clear who can be placed on the watchlist nor is it clear that there are any criteria for determining where AFR can be deployed'.[204] The Court found that too much discretion was left to individual police officers for the watchlist criteria. For example, the watchlist very broadly included 'persons where intelligence is required'.[205] There were also no limits with regard to the seriousness of offence or risk for individuals included on the watchlist.	
B. Are there clear, objective, and limited criteria for where and when FRT can be used, including mandating reasonable suspicion that persons on the watchlist will be at the location and requiring a high grade of intelligence for the police intelligence case that supports FRT use?	0 / 1
Notes: The criteria for where facial recognition could be used was not clear, objective, or limited. In the *Bridges* case, the Court of Appeal noted that, 'It is not clear who can be placed on the watchlist nor is it clear that there are any criteria for determining where AFR can be deployed'.[206] The Court found that too much discretion was left to individual police officers for the location criteria. The Court highlighted that, 'It is not said, for example, that the location must be one at which it is thought on reasonable grounds that people on the watchlist will be present'.[207]	
C. Are there clear, objective, and limited criteria concerning third-party access to the data collected or retained, including with regard to what data can be shared, with whom it can be shared, and for what specific purpose it can be shared?	0 / 1
Notes: Although there are some limits with regard to security and access, it is not clear what information can be shared with third parties such as the Home Office. SWP's DPIA states that, (a) 'only trained users will be able to access the system through a single sign on password', (b) 'operators will not have access to the watchlist data', (c) 'the images and match report are moved via an encrypted dongle which is then immediately deleted', (d) information is shared with academic partners for the sole purpose of evaluation, and the full watchlist content has not been shared with academic partners, (e) information could be shared with the Home Office Biometric Programme and the Defence Science and Technology Laboratory for the purpose of research, not law enforcement, and (f) initially information will not be collected on behalf of the Home Office, but expectations are that the system will develop at which time more formal agreements will need to be in place to regulate practices.[208]	
	0 / 3

[204] *R (Bridges) v. Chief Constable of South Wales Police, Judgement*, Court of Appeal, para. 91.

[205] *R (Bridges) v. Chief Constable of South Wales Police, Judgement*, Court of Appeal, para. 152.

[206] *R (Bridges) v. Chief Constable of South Wales Police, Judgement*, Court of Appeal, para. 91.

[207] *R (Bridges) v. Chief Constable of South Wales Police, Judgement*, Court of Appeal, para. 130.

[208] South Wales Police, 'Data Protection Impact Assessment: Automated Facial Recognition (AFR)' (11 October 2018) <https://afr.south-wales.police.uk/wp-content/uploads/2019/10/DPIA-V5.4-Live.pdf> [accessed 14 July 2022].

Necessary in a Democratic Society (Human Rights Act 1998)	Score
D. Have police identified less intrusive alternative measures and proven that FRT is strictly necessary compared to these measures using scientifically verifiable evidence?	0 / 1
Notes: SWP's documents do not transparently identify less intrusive measures nor prove that LFR is strictly necessary compared to these measures. SWP's data protection impact assessment (DPIA) states that a necessity test is required by the Human Rights Act 1998. The document states that LFR meets the core principles in policing and that the purpose of the technology is to identify persons suspected of criminality, apprehend persons wanted on warrant, and protect the most vulnerable persons in our community.[209] However, SWP did not demonstrate that the use of LFR is the least intrusive measure, which is essential for the legal test of strict necessity.	
E. Have police conducted distinct necessity tests with an evidence-based justification for each category of individuals on the watchlist?	0 / 1
Notes: SWP did not publish distinct necessity tests with an evidence-based justification for each category of individuals included on the watchlist (persons wanted on suspicion for an offence, wanted on warrant, vulnerable persons, and other persons where intelligence is required).	
F. Have police shown that FRT does not disproportionately limit the human rights of affected persons, including those who are misidentified, not on the watchlist, or impacted by unwarranted intrusions?	0 / 1
Notes: SWP's documents do not show that LFR does not disproportionately limit the rights of affected persons including those misidentified and those not on the watchlist. In the context of the proportionality test required by the Human Rights Act 1998, SWP's DPIA states that, 'It is considered appropriate to bring offenders to justice in an expeditious manner. Each deployment of AFR Locate should bring a benefit to the investigation or operation and should not be disproportionate or arbitrary. The fact that a suspected offence may be serious will not alone render intrusive actions proportionate'.[210] There is no proportionality analysis that weighs the benefits and risks of using FRT, taking into consideration the rights of those misidentified and those not on the watchlist.	
	0 / 3

[209] South Wales Police, 'Data Protection Impact Assessment', p. 11.

[210] South Wales Police, 'Data Protection Impact Assessment', p. 11–12.

Data Protection (Data Protection Act 2018)	Score
G. Before using FRT, have police carried out and published a data protection impact assessment and appropriate policy document for sensitive data processing?	1 / 1
Notes: SWP published a data protection impact assessment (DPIA) and appropriate policy document (APD) once the Data Protection Act (DPA) 2018 came into force. In the *Bridges* case, the Court of Appeal noted that, 'particularly as the Information Commissioner had expressed the view to the Divisional Court that the November 2018 Policy Document satisfied section 42(2) but ideally should be more detailed and the Divisional Court itself was uncertain whether or not it did meet the standard required by section 42 – it was entirely appropriate for the Divisional Court to make no final judgment on the point and to leave the SWP to make such revisions as might be appropriate in the light of any future guidance by the Information Commissioner'.[211] Although the DPIA and APD should have been more detailed, SWP published these documents once the DPA 2018 came into force.	
H. Beyond social media or website publishing, have police used other means to inform potential data subjects or most people in their jurisdiction in advance about when, where, why, and how FRT is being used and how they can exercise their individual rights?	0 / 1
Notes: Beyond social media and website publishing, SWP did not use other means to inform the public in advance about the use of facial recognition. There was also no clear guidance in SWP's documents on how members of the public can exercise their data protection rights such as the rights to rectification, erasure, and to object. With regard to informing the public, the SWP website notes in the FAQs that, 'All AFR Locate deployments are overt and prior to each deployment we will use social media to advertise the deployment, during the deployment signage will be used. All AFR vehicles are clearly marked'.[212] The Cardiff University report notes that ahead of the first Champions League deployment on 31 May 2017, there was a major press release by SWP: 'This was published on [22] May 2017 on South Wales Police's website and on their main Facebook page'.[213] However, there were no measures beyond social media and the police force website for informing the public in advance.	
I. Are there clear measures to ensure data subjects can exercise their individual rights including the rights to rectification, erasure, and object with clear justifications if exemptions apply?	0 / 1
Notes: There were inadequate measures to ensure that data subjects can exercise all of their individual rights. The DPIA mentions some measures to enable subject access requests: 'Where an "incorrect identification" is confirmed by human intervention officers are encouraged to record the individuals [sic.] contact details for an audit trail, in the event that a complaint or Data Protection Subject Access request is made'.[214] However, it is not clear how individuals can exercise other data protection rights such as the rights to rectification, erasure, and object.	
J. Do police check the watchlist against the data source close to the time of deployment to ensure the watchlist is accurate and up to date?	1 / 1
Notes: SWP compiles the watchlist from the data source close to the time of the deployment to ensure the watchlist is accurate and up to date. The DPIA notes that: 'Watchlists and the associated metadata are manually added to the system during the day of deployment to ensure the information is as accurate as possible. If a deployment is over a number of days a bespoke watchlist will be added at the commencement of each day of deployment'.[215] The DPIA also notes that: 'Data will be checked against core SWP databases, managed in accordance with MOPI standards'.[216]	

[211] *R (Bridges) v. Chief Constable of South Wales Police, Judgement*, Court of Appeal, para. 161.

[212] South Wales Police, *Smarter Recognition, Safer Community*.

[213] Davies, Innes, and Dawson, *An Evaluation of South Wales Police's Use of Automated Facial Recognition*, p. 39.

[214] South Wales Police, 'Data Protection Impact Assessment', p. 40.

[215] South Wales Police, 'Data Protection Impact Assessment', p. 20.

[216] South Wales Police, 'Data Protection Impact Assessment', p. 34.

Data Protection (Data Protection Act 2018) (continued)	Score
K. Are there clear measures to ensure that watchlist images are lawfully held, have a known provenance, and exclude unconvicted custody images?	0 / 1
Notes: The watchlist includes unconvicted custody images. In the DPIA, SWP notes that watchlists 'wherever possible will be born from custody images to ensure consistency of image quality and ensure the legal basis for use as defined under PACE 1984'.[217] It is not clear in what circumstances watchlist images will not be taken from the custody database and the legal basis in this case. Additionally, the use of custody images means that the watchlist includes unconvicted custody images, which are unlawful to retain.[218] In the DPIA, SWP notes that unconvicted custody images are included, as manually removing unconvicted custody images would require 25 to 35 hours, which SWP states is impracticable. This raises the concern that innocent people who are unconvicted could be identified and surveilled using LFR. Further, SWP has not taken all possible measures to remove these images. For example, there is no indication that SWP is working to automatically remove unconvicted custody images, which are unlawful to retain and thus include in the watchlist.	
L. Via direct consultation, have police proactively considered views of the public, especially marginalised communities, on the particular type of FRT and justified a disregard of the views if relevant?	0 / 1
Notes: SWP did not proactively consider views of the public, especially marginalised groups, on the use of LFR. The DPIA notes that during the September 2017 deployment at Elvis Festival, 'the community were invited to interact with the technology and ask any questions they felt relevant'.[219] The DPIA also notes that, 'An engagement vehicle has also been deployed at every Basic Command Unit (BCU) Open Day in 2017 with future deployments planned in 2018'.[220] However, there are two major concerns: (1) These engagements are not proactive consultations that occur prior to the use of LFR. (2) These engagements are not aimed at gathering views of the public, especially marginalised communities.	
M. Have police published their procurement contracts and data-sharing agreements with other parties?	0 / 1
Notes: SWP has not published their procurement contract with NEC Corporation (the LFR vendor) nor their data-sharing agreements with other entities. These documents are not available for external scrutiny.	
	2 / 7

[217] South Wales Police, 'Data Protection Impact Assessment', p. 20.

[218] *RMC and FJ v. Commissioner of Police for the Metropolis and Secretary of State for the Home Department; Home Office, Review of the Use and Retention of Custody Images* (February 2017) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/594463/2017-02-23_Custody_Image_Review.pdf> [accessed 14 July 2022].

[219] South Wales Police, 'Data Protection Impact Assessment', p 27.

[220] South Wales Police, 'Data Protection Impact Assessment', p 27.

Non-Discrimination (Human Rights Act 1998 and Equality Act 2010)	Score
N. Before using FRT, have police carried out and published an equality impact assessment?	1 / 1
Notes: SWP carried out and published an equality impact assessment (EIA) before using LFR. The EIA was conducted in April 2017 before the start of the LFR trials in May 2017. However, we note that the EIA was extremely inadequate, as SWP failed to recognise and address the risk of indirect discrimination. This issue was highlighted in the *Bridges* case, where the Court of Appeal ruled that SWP did not fulfil the Public Sector Equality Duty as SWP 'never sought to satisfy themselves, either directly or by way of independent verification, that the software program in this case does not have an unacceptable bias on grounds of race or sex'.[221] We discuss this issue further in the next section of this case study (see **Appendix D.2**).	
O. For each deployment, have police published the demographic makeup of the watchlist?	0 / 1
Notes: SWP has not published the demographic makeup of the watchlist for any of the LFR deployments. In their results, SWP only reports the size of the watchlist for each deployment.[222]	
P. For each deployment, have police published the demographic makeup of the population where FRT is used?	0 / 1
Notes: SWP has not published the demographic makeup of the population where LFR was used. There is neither quantitative nor qualitative information about the demographic makeup regarding any deployments. In their results, SWP only reports the size of the population where LFR was used for some deployments ('Faces Seen' in SWP's results).[223]	
Q. For each deployment, have police published the demographic data for arrests, stop and searches, and other outcomes resulting from the use of FRT?	0 / 1
Notes: The demographic data for arrests, stop and searches, and other outcomes has not been published. In their results, SWP only reports the number of arrests for each deployment; there is no information about other outcomes such as stop and search or report for summons.[224]	
	1 / 4

[221] *R (Bridges) v. Chief Constable of South Wales Police, Judgement*, Court of Appeal, para. 199.

[222] South Wales Police, 'List of Previous FRT Deployments'.

[223] South Wales Police, 'List of Previous FRT Deployments'.

[224] South Wales Police, 'List of Previous FRT Deployments'.

Free Expression and Assembly (Human Rights Act 1998)	Score
R. Have police assessed FRT's potential 'chilling effect' on the rights to freedom of expression and assembly to inform the legal test of 'necessary in a democratic society'?	0 / 1
Notes: Based on SWP's documents on LFR, SWP did not take any measures to assess a potential chilling effect on the rights to freedom of expression and assembly. SWP's DPIA and policy documents do not acknowledge nor address the potential impact of LFR on these rights.	
S. Do police preclude using FRT to identify those peacefully participating in an assembly?	0 / 1
Notes: FRT is not prohibited from being used to identify those peacefully participating in an assembly. In fact, on 27 March 2018, SWP used LFR to surveil a peaceful protest outside an arms fair, the Defence Procurement Research Technology Exhibition.[225] This use of FRT at a protest interferes with the rights to freedom of expression and assembly, which is concerning given that SWP provided no evidence of satisfying the legal tests of necessity and proportionality for these interferences.	
	0 / 2

D.2 Technical reliability

Algorithmic Fairness (Equality Act 2010)	Score
A. Before using FRT, have police evaluated and published the demographic makeup of the training dataset to ensure the dataset is representative of the population where it is to be used?	0 / 1
Notes: In the *Bridges* case, the Court of Appeal noted that SWP 'never sought to satisfy themselves, either directly or by way of independent verification, that the software program in this case does not have an unacceptable bias on grounds of race or sex'.[226] Before or during the LFR deployments, there was no evaluation of the demographic makeup of the training dataset. The precise makeup of the training dataset remains unknown due to commercial sensitivity, as noted in the *Bridges* case. However, without this information about the training dataset, it would be challenging for SWP to assess whether FRT is biased.	
B. Before using FRT, have police evaluated and published FRT's performance across demographic groups, in different conditions that match FRT's operational use, to ensure FRT performs well and similarly across the population?	0 / 1
Notes: In the *Bridges* case, the Court of Appeal noted that SWP 'never sought to satisfy themselves, either directly or by way of independent verification, that the software program in this case does not have an unacceptable bias on grounds of race or sex'.[227] Before or during the LFR deployments, there was no evaluation of LFR's performance across demographic groups in conditions that matched the operational use of LFR. The SWP's equality impact assessment (EIA) itself did not acknowledge the risk of differential LFR performance across demographic groups.	
	0 / 2

[225] Big Brother Watch, Face Off; Apple, 'South Wales Police Under Fire'.

[226] *R (Bridges) v. Chief Constable of South Wales Police, Judgement*, Court of Appeal, para. 199.

[227] *R (Bridges) v. Chief Constable of South Wales Police, Judgement*, Court of Appeal, para. 199.

Robust Practice (Data Protection Act 2018)	Score
C. Are there safeguards precluding the use of FRT with an unsuitable low-quality probe or watchlist image?	0 / 1
Notes: There are no safeguards precluding the use of LFR with unsuitable low-quality images. The Cardiff University evaluation report on SWP's trials notes that poor-quality images were uploaded onto the LFR system, which resulted in a small number of people becoming frequent 'hitters'.[228] SWP's Standard Operating Procedure Document also confirms this lack of safeguards to preclude the use of poor-quality images. Even though the document indicates what is a usable image (e.g. front-facing, plain background), the LFR system can still search unsuitable images on which the system would have a poor performance, likely resulting in misidentifications.	
D. Have police pre-established and met thresholds for the FRT system's accuracy (precision, false positive rate, true positive rate) to inform the legal test of strict necessity for personal data processing?	0 / 1
Notes: SWP's documents do not indicate any pre-established thresholds for the LFR system's accuracy. Furthermore, the number of true positives is unknown for many deployments, and it is unclear whether the true positive rate was measured for all deployments.[229]	
	0 / 2

Deployment Performance (Equality Act 2010)	Score
E. Does FRT perform well (precision, false positive rate, true positive rate) and similarly across demographic groups?	0 / 1
Notes: LFR does not perform well nor similarly across demographic groups: (1) LFR had a poor precision of 24%, meaning that out of the matches that LFR generated, only 24% were correct. (2) There was a higher false positive rate for the female alerts (82%) compared to the false positive rate of the male alerts (66%). We provide details of these calculations: (1) Across 50 deployments from September 2017 to April 2019, SWP's use of FRT yielded 88 verifiably correct matches ('Positive Interventions' in SWP's results) from a total of 364 FRT-generated matches ('Positive Alerts' and 'Incorrect Alerts' in SWP's results).[230] This means that the precision of matches was 88/364 = 24%. (2) The *Bridges* case provided the following demographic data with regard to LFR performance.[231] For all deployments from September 2017 to June 2018, 290 alerts were generated. 82 (28%) were true positives and 208 (72%) were false positives. 188 of the alerts were males (65%). Of the 188 male alerts, 64 (34%) were true positives and 124 (66%) were false positives. In relation to females, of 102 alerts, 18 (18%) were true positives and 84 (82%) were false positives. With regard to ethnicity, of true positives (82), 98% were 'white north European'. Of the false positives (208), 98.5% were 'white north European'.[232]	
	0 / 1

[228] Davies, Innes, and Dawson, *An Evaluation of South Wales Police's Use of Automated Facial Recognition*, p. 23.

[229] South Wales Police, 'List of Previous FRT Deployments'; Davies, Innes, and Dawson, *An Evaluation of South Wales Police's Use of Automated Facial Recognition*.

[230] South Wales Police, 'List of Previous FRT Deployments'.

[231] *R (Bridges) v. Chief Constable of South Wales Police, Judgement*, Court of Appeal, para. 187–189.

[232] *R (Bridges) v. Chief Constable of South Wales Police, Judgement*, Court of Appeal, para. 189.

D.3 Human decision-making

Human Review	Score
A. Is there a transparent evaluation that shows human review of the FRT matches is reliable, given the accuracy of officer-verified matches and the amount of time an officer has to review an FRT match?	0 / 1
Notes: Human review of LFR had a 69% precision, meaning that out of the interventions based on human review of LFR, only 69% of individuals were correctly identified. Across 50 deployments from September 2017 to April 2019, there were 127 individuals stopped based on LFR matches verified by an officer ('Positive Interventions' and 'Incorrect Interventions' in SWP's results), and 88 of these individuals were confirmed to be correctly matched once an identity check took place ('Positive Interventions' in SWP's results).[233] This means that the precision of human review was 88/127 = 69%. Additionally, there is no transparent evaluation of the amount of time officers had to review LFR matches. The Cardiff University evaluation report only comments on the amount of time officers had to review matches for retrospective FRT ('AFR Identify'). Given the real-time nature of LFR, it is likely that officers did not have a significant amount of time to review FRT matches.	
	0 / 1

[233] South Wales Police, 'List of Previous FRT Deployments'.

Preparation	Score
B. Is training for the particular type of FRT mandated for police officers using the technology?	0 / 1
Notes: Formal training was not required for police officers using FRT for the initial trial deployments. Cardiff University's evaluation report on SWP's FRT deployments between May 2017 and March 2018 states that there was some training for the first Champions League deployment. However, the report notes that following this first deployment, 'no other formal training was provided to operators. Whenever someone new worked on a deployment, they were simply given brief instructions on how to operate the system by an operator who had used it before. This means that many operators are currently using the system without formal training'.[234] SWP's DPIA dated October 2018 indicates that training was mandated for staff operating the FRT system; two-day training was provided to administrators and a half-day training was provided to users of the FRT system.[235] This suggests that training was required for the later trial deployments.	
C. Are there clear standards for technical training on using FRT, data protection training, and training on risks including differential treatment, function creep, and unwarranted intrusions?	0 / 1
Notes: The training provided was primarily technical, and there was no training on data protection and the risks of FRT. Cardiff University's evaluation report on SWP's FRT deployments between May 2017 and March 2018 states that there was some technical training for the first deployment. The vendor NEC provided a basic training session on how to use the FRT system. Additionally, the day before the deployment, officers on the FRT project team led a familiarisation session: 'The purpose here was to brief operators on the more practical elements of the deployment and to explain how the technology would fit into the wider policing operation'.[236] For later FRT deployments after March 2018, the DPIA dated October 2018 indicates that: 'Staff have the necessary training to operate the systems including the location of any remote, fixed or flexible cameras and their remit'.[237] Thus, for all deployments from 2017 to 2019, the training provided was technical and did not include training on data protection and the risks of FRT such as differential treatment, function creep, and unwarranted intrusions.	
D. Has there been a documented non-operational research trial of FRT with informed consent from participants before the operational use of FRT for policing?	0 / 1
Notes: There has not been a documented non-operational trial of FRT before its operational use. The Cardiff University report notes that they carried out a small-scale field trial with seven volunteers during a deployment (Wales v. Italy Six Nations match) in March 2018. However, this trial to test the technology occurred after 16 operational trial deployments and was also limited in scope.	
	0 / 3

[234] Davies, Innes, and Dawson, *An Evaluation of South Wales Police's Use of Automated Facial Recognition*, p. 16.

[235] South Wales Police, 'Data Protection Impact Assessment', p. 36.

[236] Davies, Innes, and Dawson, *An Evaluation of South Wales Police's Use of Automated Facial Recognition*, p. 16.

[237] South Wales Police, 'Data Protection Impact Assessment', p. 14.

Accountability	Score
E. Are there clear measures for police to document cases of harm resulting from the use of FRT such as differential treatment, function creep, or unwarranted intrusions?	0 / 1
Notes: There are no clear measures for police to report harm. SWP's deployment results do not include any evaluations of differential treatment or function creep.[238] While the deployment results indicate the number of incorrect police interventions, there is no public documentation of what kind of unwarranted intrusions these interventions resulted in (e.g. their images being retained, their fingerprints being scanned, stop and search).	
F. Do police have a whistleblower protection policy to protect persons who reveal FRT misuse?	0 / 1
Notes: There was no whistleblower protection policy in place from the start of the FRT deployments. SWP established a whistleblower protection policy in March 2019, which was after the majority of the LFR deployments.[239]	
G. Is there a clear redress mechanism (beyond judicial review and usual complaint procedures) for harmed individuals and groups to participate in an investigation into police use of FRT?	0 / 1
Notes: Based on SWP's documents, there is no clear redress mechanism for those harmed by the use of LFR. In the context of accountability, SWP's DPIA notes that, 'South Wales Police have developed a detailed governance structure to ensure that there is a sound accountability and engagement with key stakeholders. These include bi-monthly AFR Project Boards along with bi-monthly AFR Strategic Partnership Boards which involve key stakeholders and regulators. South Wales Police are also represented at the "Forensic Oversight Board" as detailed within the Home Office Biometric Strategy'.[240] However, there are no clear mechanisms for harmed persons to participate in an investigation into SWP's use of LFR. This deficiency is confirmed by the House of Lords Justice and Home Affairs Committee report on new technologies in the justice system that highlights the lack of recourse for people harmed by the use of technologies such as FRT.[241]	
H. Are there clear measures to ensure that the redress mechanism is procedurally fair?	0 / 1
Notes: There are no clear measures to ensure a procedurally fair redress mechanism; there is no clear redress mechanism for harmed persons in the first place.	
	0 / 4

[238] South Wales Police, 'List of Previous FRT Deployments'.

[239] 'Whistleblowing: Guidance & Procedure Summary' (14 March 2019) <https://www.south-wales.police.uk/SysSiteAssets/media/downloads/south-wales/about-us/policies-and-procedures/english/whistleblowing.pdf> [accessed 14 July 2022].

[240] South Wales Police, 'Data Protection Impact Assessment', p. 12.

[241] House of Lords, Justice and Home Affairs Committee, *Technology Rules?*, p. 37.

D.4 Expertise and oversight

<table>
<tr><th>Ethics Committee</th><th>Score</th></tr>
<tr><td>A. Is regular oversight from an ethics committee mandated throughout the life of the FRT project?</td><td>0 / 1</td></tr>
<tr><td colspan="2"><b>Notes:</b> Even though SWP engaged with the SWP Independent Ethics Committee, there was a lack of regular oversight from the committee throughout the life of the FRT project. Note that the FRT trials started in May 2017. The DPIA notes that SWP consulted the SWP Independent Ethics Committee through 'early engagement over the concept of implementation and its engagement with privacy against the provision of safer communities'.[242] When we examined the SWP Joint Independent Ethics Committee's meeting notes that were published starting from September 2018, we found that facial recognition was only mentioned in three meetings: September 2018, December 2018, and March 2019.[243] At two of these meetings (September 2018 and March 2019), there was a mention of FRT but no discussion or oversight about its use by SWP. At only one of these meetings (December 2018) was there a discussion about FRT, yet this discussion itself is not published. This lack of transparency makes it challenging to know the extent to which oversight was provided during the meeting. There is also no published evidence of oversight from the committee prior to or at the start of the FRT trials in May 2017, even though the committee was formed in 2015.[244]</td></tr>
<tr><td>B. Are there clear processes for the committee to influence if and how FRT is implemented, including the power of veto for the FRT project?</td><td>0 / 1</td></tr>
<tr><td colspan="2"><b>Notes:</b> The SWP Joint Independent Ethics Committee is advisory, and there are no clear processes for the committee to influence if and how FRT is implemented, including the power of veto. The specific feedback from the committee on the implementation of FRT is not published, and it is not clear whether this feedback influenced if and how FRT was implemented. The committee's Terms of Business are not published, but the SWP website states that the committee provides advice, support and assistance.[245] Thus, the nature of the committee is advisory and likely lacks decision-making power that includes the power of veto.</td></tr>
</table>

[242] South Wales Police, 'Data Protection Impact Assessment', p. 25.

[243] South Wales Police, 'Our Vision, Values, and Ethics' <https://www.south-wales.police.uk/police-forces/south-wales-police/areas/about-us/about-us/our-vision-values-and-ethics/> [accessed 14 July 2022]; South Wales Police Joint Independent Ethics Committee, 'Meeting Minutes, 12 September 2018' <https://www.south-wales.police.uk/SysSiteAssets/media/downloads/force-content/south-wales/independent-ethics-committee/independent-ethics-committee-meeting-minutes-october-2018.pdf> [accessed 14 July 2022]; South Wales Police Joint Independent Ethics Committee, 'Meeting Minutes, 12 December 2018' <https://www.south-wales.police.uk/SysSiteAssets/media/downloads/force-content/south-wales/independent-ethics-committee/independent-ethics-committee-meeting-minutes-december-2018.pdf> [accessed 14 July 2022]; South Wales Police Joint Independent Ethics Committee, 'Meeting Minutes, 27 March 2019' <https://www.south-wales.police.uk/SysSiteAssets/media/downloads/force-content/south-wales/independent-ethics-committee/independent-ethics-committee-meeting-minutes-March-2019.docx> [accessed 14 July 2022].

[244] Alun Michael, *Police and Crime Commissioner for South Wales/De Cymru Comisiynydd yr Heddlu a Throseddu: Annual Report*, 2015–2016 <http://pcclivewww.blob.core.windows.net/wordpress-uploads/2151-SWPCC-Annual-Report-2015-2016-English.pdf> [accessed 14 July 2022].

[245] South Wales Police, 'Our Vision, Values, and Ethics'.

Ethics Committee (continued)	**Score**
C. Is the committee an independent body from police organisations with members having non-policing backgrounds and with safeguards to ensure the committee's sustainability even without political support?	0 / 1
Notes: The SWP Joint Independent Ethics Committee is not an independent body, as it is situated within South Wales Police. Although the committee includes some independent members, the committee also includes police officers (Chief Officer and Chief Superintendent).[246] Further, the majority of committee meeting attendees were members of police service organisations. Across the September 2018, December 2018, and March 2019 meetings where LFR was mentioned, there were 24 different individuals in attendance, 15 (63%) of which were members of SWP and 17 (71%) were either a member of SWP or the South Wales Police and Crime Commissioner.[247] Finally, the committee's Terms of Business are not published, and it is not clear what safeguards are in place to ensure the committee's sustainability.	
D. Is the committee diverse in terms of demographic makeup and independent expertise in human rights, equality, and data protection?	0 / 1
Notes: The demographic diversity of the SWP Joint Independent Ethics Committee is not published. We also researched the backgrounds of the persons in attendance during the September 2018, December 2018, and March 2019 meetings and found that there were no independent experts in human rights, equality, and data protection in attendance.[248] Based on recruitment materials for the appointment of members to the committee, there is no indication that demographic diversity is considered in the selection of members nor that expertise in human rights, equality, or data protection is considered.[249]	
E. Are detailed meeting minutes published, including briefing papers, discussions, and conclusions?	0 / 1
Notes: Although the committee's minutes are published, detailed discussions and briefing papers from the meetings where LFR was mentioned have not been made public. For example, the December 2018 minutes note that a report on the implementation of LFR and its ethical issues was finalised and forwarded to the Police and Crime Commissioner.[250] However, there is no publication of the committee's discussions on the report nor a publication of the report itself. The minutes also note that a presentation on the ethics of LFR was given at the NPCC Professional Standards and Ethics national conference. However, this presentation has also not been made public.	
	0 / 5

[246] South Wales Police, 'Our Vision, Values, and Ethics'.

[247] South Wales Police Joint Independent Ethics Committee, 'Meeting Minutes, 12 September 2018'; South Wales Police Joint Independent Ethics Committee, 'Meeting Minutes, 12 December 2018'; South Wales Police Joint Independent Ethics Committee, 'Meeting Minutes, 27 March 2019'.

[248] South Wales Police Joint Independent Ethics Committee, 'Meeting Minutes, 12 September 2018'; South Wales Police Joint Independent Ethics Committee, 'Meeting Minutes, 12 December 2018'; South Wales Police Joint Independent Ethics Committee, 'Meeting Minutes, 27 March 2019'.

[249] South Wales Police Corporate Services, *Briefing Pack: Independent Ethics Committee Members* (May 2022) <https://www.south-wales.police.uk/SysSiteAssets/media/downloads/south-wales/about-us/careers/hr-documents/2022-06-08-iec-information-pack-new.pdf> [accessed 15 July 2022]; South Wales Police and Crime Commissioner and Chief Constable, 'Appointment of Members to *The Independent* Ethics Committee' (July 2022) <https://www.south-wales.police.uk/SysSiteAssets/media/downloads/south-wales/about-us/careers/hr-documents/job-description-june-22-update.pdf> [accessed 15 July 2022]; South Wales Police and Crime Commissioner and Chief Constable, 'Person Specification – Independent Ethics Committee' (2017) <https://www.south-wales.police.uk/SysSiteAssets/media/downloads/south-wales/about-us/careers/hr-documents/person-specification-2020.pdf> [accessed 15 July 2022].

[250] South Wales Police Joint Independent Ethics Committee, 'Meeting Minutes, 12 December 2018'.

Civil Society and Experts	Score
F. Are there transparent, proactive consultations with civil society and independent experts on the particular type of FRT?	0 / 1
Notes: There were no transparent consultations with civil society before or during the use of FRT. SWP provides a consultation log within their DPIA.[251] Based on the log, SWP primarily consulted with other police forces, government bodies, policing bodies, and a police science academic institution. The DPIA also states that, 'Wider debate has been sought at the Surveillance Camera Commissioner's Advisory Counsel held on [22] May 2018. In attendance were representatives from Liberty and Big Brother Watch. South Wales Police were invited to attend this meeting and provide an overview of the use of the technology. Concerns over its use were raised by both representatives from Big Brother Watch and Liberty. Time was taken after this meeting to discuss the use of the technology in more detail with representatives from Big Brother Watch'.[252] However, it is not clear what concerns were raised and whether SWP took these concerns into account in their use of LFR. Additionally, these engagements were not proactive and occurred after numerous LFR deployments already took place.	
G. Are police required to consider the advice from consultations and transparently explain the outcomes, including providing a justification if the advice is not followed?	0 / 1
Notes: There were no clear requirements that SWP must consider the advice from consultations, and there were no requirements for them to transparently explain the outcomes. In the context of consultations, SWP mentions in the DPIA that there were professional discussions and advice provided from particular entities.[253] However, the outcome of these consultations is not clear. It is unknown whether the advice was followed and the reason in the case that the advice was not followed.	
	0 / 2

Community Engagement	Score
H. Are there clear, proactive processes for the public, especially marginalised communities, to influence if and how FRT is implemented?	0 / 1
Notes: There were no clear, proactive processes for the public to influence if and how FRT was implemented. SWP's DPIA mentions their communication strategy to inform the public about the use of FRT: 'Social Media has been used extensively to inform the community of each deployment. Where possible the location of the vehicle has also been advertised, with the public invited to "take a look" at the technology. Social media has also been used by both the Project team and Chief Officers to participate in a healthy debate over the necessity and ethicacy [sic] of its use'.[254] These efforts help inform the public often during deployments but do not create avenues for the public, especially marginalised communities, to share their concerns and influence the FRT project during its concept and design stages.	
I. Are all FRT materials accessible to people with disabilities and provided in immigrant languages?	0 / 1
Notes: The LFR documents on the SWP website may not be accessible to people with disabilities. There is no accessibility statement that indicates the extent to which the website is accessible.[255] The documents on LFR are also not provided in immigrant languages. These accessibility issues can pose barriers to certain communities and make it difficult to understand the use and impact of LFR.	
	0 / 2

[251] South Wales Police, 'Data Protection Impact Assessment'.

[252] South Wales Police, 'Data Protection Impact Assessment', p. 26.

[253] South Wales Police, 'Data Protection Impact Assessment', pp. 25–26.

[254] South Wales Police, 'Data Protection Impact Assessment', p. 27.

[255] South Wales Police, *Smarter Recognition, Safer Community*.

E. Metropolitan Police Service's Trial of Live Facial Recognition

Police Force: Metropolitan Police Service (MPS)

Facial Recognition Type: Live Facial Recognition (LFR)

LFR Deployment Dates: Trial deployments from August 2016 to February 2019

Audit Evaluation Date: July 2022

Key Resources Used: MPS DPIA, **MPS Legal Mandate**, **MPS Report**, **Essex University Report**

The next case study is of the operational trial deployments of live facial recognition (LFR) conducted by the Metropolitan Police Service (MPS) from August 2016 to February 2019. We build upon a study conducted by University of Essex researchers on the human rights compliance of these trials. Their report concludes that the trials would likely 'be held unlawful if challenged before the courts' given the absence of clear guidance on who was included in a watchlist and the failure to establish that LFR was 'necessary in a democratic society' as required by human rights law.[256] We found additional concerns related to discrimination and oversight.

While MPS published some demographic data in their results, they did not record the demographic breakdown for engagements, stop and searches, arrests, and other outcomes resulting from the use of LFR. This makes it hard to evaluate whether LFR perpetuates racial profiling. There was also no published evaluation of racial or gender bias in the technology. MPS conducted an internal evaluation but did not disclose the results. This lack of transparency makes it difficult for outside stakeholders to assess the comprehensiveness of the evaluation.

Since the trial deployments have ended, MPS has frequently pointed to an evaluation undertaken by the National Institute of Standards & Technology.[257] However, citing this evaluation can be misleading: even though the evaluation shows a high accuracy, it was conducted with high-quality standardised images rather than low-quality wild images on which LFR was used.[258] The absence of a published evaluation in conditions that match LFR's use is especially concerning given that the same technology used by MPS misidentified and led to wrongful arrests of Black men in the United States.[259]

With regard to oversight, MPS engaged with the London Policing Ethics Panel (LPEP). However, transparent oversight began after several deployments rather than starting from the concept stage of the trial. Even though MPS responded to the panel's recommendations, the panel was advisory and MPS was not required to act upon the recommendations. There were also no experts in human rights, equality, or data protection on the panel, even though this has been documented as crucial for the oversight of LFR.

[256] Fussey and Murray, *Independent Report*. p. 6.

[257] Ephgrave, 'MPS Response'; Metropolitan Police Service, 'Equality Impact Assessment'; Grother, Ngan, and Hanaoka, 'Face Recognition Vendor Test'.

[258] Currently, MPS is testing the performance of LFR with the National Physical Laboratory during operational deployments. This evaluation is expected to complete in the third quarter of 2022, significantly after numerous deployments have already occurred. The data collected during the evaluation may also be shared with the UK law enforcement community and its partners, raising concerns about broad access and potential function creep.

[259] MPS procured its LFR technology from the company NEC Corporation. NEC's facial recognition technology was used by police in the United States in 'cases of Black men wrongfully accused of crimes they did not commit in Detroit and New Jersey, as the underlying algorithm for facial recognition provided by contractor DataWorks Plus', 'NEC Corp'. See also: Hill, 'Wrongfully Accused'; Coulter, 'A Black Man Spent 10 Days in Jail'.

Below we provide the full audit scorecard for this case study, which includes the score and accompanying explanation for each question.

E.1 Legal standards

In Accordance with the Law (Human Rights Act 1998)	**Score**
A. Are there clear, objective, and limited criteria for who can be included in the watchlist, including with regard to the image source and the seriousness of offence or risk?	0 / 1
Notes: The watchlist criteria was not limited in terms of the seriousness of offence or risk. In the DPIA, MPS established that their intended use of LFR was to identify: (a) 'individuals shown as wanted by the police and the courts', (b) 'individuals who present a risk of harm to themselves and others', (c) 'wanted individuals or those with conditions not to attend an area based on intelligence and crime analysis', and (d) 'individuals who may be at risk or vulnerable'.[260] These criteria lack limitations on the type of offence or risk. With regard to the image source, the DPIA indicates that 'Images, usually taken from the custody imaging database or from images provided from specific sources of intelligence, for example from persons reporting vulnerable missing persons, will be uploaded on to the LFR watch list data base'.[261] There is no clear limitation that the images must be lawfully held.	
B. Are there clear, objective, and limited criteria for where and when FRT can be used, including mandating reasonable suspicion that persons on the watchlist will be at the location and requiring a high grade of intelligence for the police intelligence case that supports FRT use?	0 / 1
Notes: The location criteria for LFR were not clear and limited. The DPIA notes that, 'A total of 10 events representing different physical and policing environments were chosen in order to assess under what conditions LFR could be most efficiently deployed'.[262] While MPS' report provides some information about these different environments, it is not clear how and why each event was selected. For example, one environment identified by MPS was 'an uncontrolled flow of a high density of subjects'.[263] However, it is not clear why the Notting Hill Carnival, as compared to other events, was chosen to represent this environment. More importantly, there was no requirement of reasonable suspicion that persons on the watchlist were at the event. Finally, while the DPIA indicates that there is an intelligence case to support each deployment, the grade or quality of the intelligence is not clear.	
C. Are there clear, objective, and limited criteria concerning third-party access to the data collected or retained, including with regard to what data can be shared, with whom it can be shared, and for what specific purpose it can be shared?	1 / 1
Notes: There are clear limits with regard to access; information is not shared beyond police staff working on the FRT project. MPS' DPIA states that, 'There is no retrospective searching or sharing of information'.[264] The DPIA also notes that, 'Officers/ Staff compiling the watch lists are briefed in respect of watch list circulation and have been informed that this sensitive data must not be disclosed outside the operational command team, deployable officers and technical support staff'.[265] With regard to security measures, the DPIA notes that watchlist images are 'sent over the closed access point to password protected hand held devices'.[266]	
	1 / 3

[260] Nelson, 'Metropolitan Police Service Privacy Impact Assessment', p. 2.
[261] Nelson, 'Metropolitan Police Service Privacy Impact Assessment', p. 3.
[262] Nelson, 'Metropolitan Police Service Privacy Impact Assessment', p. 2.
[263] National Physical Laboratory and Metropolitan Police Service, *Metropolitan Police Service Live Facial Recognition Trials*, p. 20.
[264] Nelson, 'Metropolitan Police Service Privacy Impact Assessment', p. 3.
[265] Nelson, 'Metropolitan Police Service Privacy Impact Assessment', p. 14.
[266] Nelson, 'Metropolitan Police Service Privacy Impact Assessment', p. 3.

Necessary in a Democratic Society (Human Rights Act 1998)	Score
D. Have police identified less intrusive alternative measures and proven that FRT is strictly necessary compared to these measures using scientifically verifiable evidence?	0 / 1
Notes: MPS did not prove that LFR is strictly necessary compared to less intrusive alternative measures. The Legal Mandate states that: 'This approach is less intrusive than other methods of tracing wanted persons. It is less resource intensive which will save police time and money and allow police to concentrate resources on other priorities […] Previously, other methods have been employed and proved to be inadequate. These methods have included visiting addresses of the wanted person or their families and associates, developing police intelligence databases or using intelligence generated from parties to facilitate locating them. LFR is likely to be more effective and efficient as it does not rely on information sharing with other agencies'.[267] However, there is no scientifically verifiable evidence showing that LFR is 'necessary in a democratic society' compared to these alternative methods. Note that the 'necessary in a democratic society' test is not a test of LFR's usefulness, but involves addressing LFR's interference with human rights in a democratic society.	
E. Have police conducted distinct necessity tests with an evidence-based justification for each category of individuals on the watchlist?	0 / 1
Notes: MPS did not conduct distinct necessity tests with an evidence-based justification for each category of individuals on the watchlist (individuals wanted by the police, individuals wanted by the courts, individuals who present a risk of harm, individuals with conditions not to attend an area, vulnerable individuals). The University of Essex evaluation of MPS' LFR trial notes this lack of distinct necessity tests for each category of individuals on the watchlist.[268]	
F. Have police shown that FRT does not disproportionately limit the human rights of affected persons, including those who are misidentified, not on the watchlist, or impacted by unwarranted intrusions?	0 / 1
Notes: The University of Essex evaluation of MPS' LFR trial notes that their necessity and proportionality analysis 'fails to adequately take into account the impact that the deployment of LFR technology has on those individuals who do not appear on the watchlist but who are subject to data processing by LFR technology, or the impact on those individuals who are incorrectly identified as being on the watchlist'.[269]	
	0 / 3

[267] Galopin and Nelson, 'Live Facial Recognition, (LFR) MPS Legal Mandate', pp. 5–6.

[268] Fussey and Murray, *Independent Report*, p. 58.

[269] Fussey and Murray, *Independent Report*, p. 60.

Data Protection (Data Protection Act 2018)	Score
G. Before using FRT, have police carried out and published a data protection impact assessment and appropriate policy document for sensitive data processing?	0 / 1
Notes: MPS carried out and published a data protection impact assessment dated July 2018. Version 1.0 of an appropriate policy document for sensitive data processing within FRT deployments was created on 10 February 2020.[270] An FOI request confirms that this document is MPS' first appropriate policy document for the use of LFR.[271] This indicates that the appropriate policy document was created and published more than a year after it was required in 2018 by the Data Protection Act 2018.	
H. Beyond social media or website publishing, have police used other means to inform potential data subjects or most people in their jurisdiction in advance about when, where, why, and how FRT is being used and how they can exercise their individual rights?	0 / 1
Notes: Beyond social media and website publishing, MPS used public information leaflets to inform people about the use of FRT. However, these leaflets were not distributed in advance but rather at the FRT trial deployments themselves. Further, the University of Essex report notes that, 'There has been some debate over the degree to which these leaflets were distributed to the public. Some civil society groups have stated that very few leaflets were given out at test deployments they observed. Researchers witnessed uniformed officers distributing this information on a regular basis'.[272] Moreover, while leaflets included information about the time and location of FRT use, there was less clarity over why FRT was being deployed and no indication of how individuals could exercise their data protection rights.[273]	
I. Are there clear measures to ensure data subjects can exercise their individual rights including the rights to rectification, erasure, and object with clear justifications if exemptions apply?	0 / 1
Notes: MPS' DPIA does not indicate clear procedures to enable data subjects (i.e. the public) to exercise their individual rights including the rights to access, rectification, and erasure. It is not articulated how the use of LFR impacts these rights and how the public can exercise them. Additionally, with regard to the right to object, the University of Essex evaluation of MPS' LFR trial notes issues with the public's capacity to refuse the use of LFR; for example, at the Stratford deployment, avoiding LFR cameras required a walking detour of an additional 18 minutes.[274] There were also concerns that avoiding LFR cameras might have been seen as suspicious behaviour, possibly undermining the right to object.[275]	

[270] Metropolitan Police Service, 'Appropriate Policy Document for Sensitive Data Processing Within Live Facial Recognition Deployments' (10 February 2021) <https://www.met.police.uk/SysSiteAssets/media/downloads/central/services/accessing-information/facial-recognition/appropriate-policy-document.pdf> [accessed 15 July 2022].

[271] Metropolitan Police Service, Information Rights Unit, 'Response to Freedom of Information Request: Live Facial Recognition Deployments, ref. 01FOI/22/024489' (4 June 2022) <https://drive.google.com/file/d/1xl7W5ZDopekq-gVzwjZysiOtgiBYttuz/view?usp=sharing> [accessed 15 July 2022].

[272] Fussey and Murray, *Independent Report*, p. 92.

[273] Fussey and Murray, *Independent Report*, p. 93.

[274] Fussey and Murray, *Independent Report*, p. 12.

[275] Fussey and Murray, *Independent Report*, p. 12.

Data Protection (Data Protection Act 2018) (continued)	Score
J. Do police check the watchlist against the data source close to the time of deployment to ensure the watchlist is accurate and up to date?	0 / 1
Notes: The watchlist was not always checked against the data source close to the time of the deployment, resulting in watchlist inaccuracy on several occasions. The DPIA notes that, 'Watch lists are compiled some time prior to deployment […] and are reviewed again no more than 2 days prior to the operation to ensure that it only contains relevant and actionable data'.[276] However, the University of Essex evaluation highlights issues related to accuracy that arose.[277] (a) The Essex evaluation notes that the aforementioned statement in the DPIA about reviewing the watchlist within two days of deployment was removed ahead of the 2019 Romford deployments, where an individual was stopped based on outdated information, but 'he had already been dealt with by the criminal justice system in the time between watchlist compilation and the LFR test deployment, and so should not have been included on the watchlist'.[278] (b) The Essex evaluation discusses the first 2018 Soho test deployment, which was covered by the original DPIA committing to review the watchlist within two days of deployment. At this Soho deployment, an individual was also stopped on the basis of outdated information. The Essex evaluation concludes that, 'The difficulties of assembling large watchlists and way this issue played out in the incidents highlighted above severely restrict the likelihood that this commitment [to review the watchlist within two days of deployment] could be upheld'.[279]	
K. Are there clear measures to ensure that watchlist images are lawfully held, have a known provenance, and exclude unconvicted custody images?	0 / 1
Notes: There are no clear measures to ensure that watchlist images exclude unconvicted custody images. The DPIA states that: 'Watch list images are sourced from the custody imaging system'.[280] However, there is no acknowledgement of the risk that unconvicted custody images, which are unlawful to retain, might be included in the watchlist.	
L. Via direct consultation, have police proactively considered views of the public, especially marginalised communities, on the particular type of FRT and justified a disregard of the views if relevant?	0 / 1
Notes: There is no indication that MPS considered the views of the public, especially marginalised groups, on the use of LFR. The DPIA includes a very brief section on consultation results that does not indicate which stakeholders were consulted: 'A stakeholder engagement strategy has been developed in order to both identify key stakeholders and formulate an effective means of communicating and developing trust and confidence in LFR technology and its application as a police tactic. Stakeholder engagement strategy has been developed and inter laced with Press and Media and Risk Management strategies'.[281]	
M. Have police published their procurement contracts and data-sharing agreements with other parties?	0 / 1
Notes: MPS has not published its procurement contract with NEC nor its data-sharing agreements with other entities. These documents are not available for external scrutiny.	
	0 / 7

[276] Nelson, 'Metropolitan Police Service Privacy Impact Assessment', p. 14.

[277] Fussey and Murray, *Independent Report*, p. 83–85.

[278] Fussey and Murray, *Independent Report*, p. 84.

[279] Fussey and Murray, *Independent Report*, p. 85.

[280] Nelson, 'Metropolitan Police Service Privacy Impact Assessment', p. 3.

[281] Nelson, 'Metropolitan Police Service Privacy Impact Assessment', p. 17.

Non-Discrimination (Human Rights Act 1998 and Equality Act 2010)	Score
N. Before using FRT, have police carried out and published an equality impact assessment?	0 / 1
Notes: The MPS did not carry out an EIA for the trial deployments, as indicated by MPS' response to a freedom of information request.[282]	
O. For each deployment, have police published the demographic makeup of the watchlist?	0 / 1
Notes: MPS' report on the ten trial deployments includes some information about the demographic makeup of the watchlist.[283] For each of the last five deployments, the distribution across perceived ethnicity for the watchlist is shown via a pie chart. However, there is no demographic information about ethnicity for the watchlists of the first five deployments, and there is no demographic information about gender for the watchlist of any deployment.	
P. For each deployment, have police published the demographic makeup of the population where FRT is used?	0 / 1
Notes: MPS' report on the ten trial deployments includes some information about the distribution across demographic groups on which FRT is used.[284] For each of the last five deployments, the distribution across perceived ethnicity for the crowd is shown via a pie chart. However, there is no demographic information for the first five deployments.	
Q. For each deployment, have police published the demographic data for arrests, stop and searches, and other outcomes resulting from the use of FRT?	0 / 1
Notes: MPS has not published the demographic data for engagements, stop and searches, arrests, and other outcomes resulting from the use of FRT. An FOI request indicates that MPS did not record and therefore does not hold the demographic data for engagements resulting from the use of FRT (either based on true matches or false matches).[285]	
	0 / 4

[282] Metropolitan Police Service, 'Response to Freedom of Information Request: MPS's Trial of Live Facial Recognition Technology, ref. 01.FOI.19.011245' <https://www.met.police.uk/foi-ai/metropolitan-police/disclosure-2019/september/mps-trial-live-facial-recognition-technology/> [accessed 15 July 2022].

[283] National Physical Laboratory and Metropolitan Police Service, *Metropolitan Police Service Live Facial Recognition Trials*.

[284] National Physical Laboratory and Metropolitan Police Service, *Metropolitan Police Service Live Facial Recognition Trials*.

[285] Metropolitan Police Service, Information Rights Unit, 'Response to Freedom of Information Request: MPS' Use of Live Facial Recognition, ref. 01FOI/22/024139' (17 June 2022) <https://drive.google.com/file/d/1wEk-2FVtUGetiaKsOa1HGTZ9qQ4XNa1B/view?usp=sharing> [accessed 15 July 2022].

Free Expression and Assembly (Human Rights Act 1998)	Score
R. Have police assessed FRT's potential 'chilling effect' on the rights to freedom of expression and assembly to inform the legal test of 'necessary in a democratic society'?	0 / 1
Notes: MPS did not assess a potential chilling effect. During the time of the trial deployments, MPS' legal mandate did not acknowledge a potential chilling effect, nor LFR's interference with the human rights to freedom of expression and assembly.[286] In May 2019, after the trial deployments, London Policing Panel reported the results of a survey with the local community and found that 19% would stay away from LFR monitored events'.[287] Notably, the percentage was higher among young people and communities of colour: 38% of 16–24-year-olds, 29% of Asians, 23% of Blacks and 28% of Mixed ethnic groups agreed that they would stay away from LFR monitored events. MPS' most recent legal mandate on LFR does not take these results into account.[288]	
S. Do police preclude using FRT to identify those peacefully participating in an assembly?	0 / 1
Notes: LFR is not prohibited from being used to identify those peacefully participating in an assembly. MPS' legal mandate did not acknowledge LFR's interference with the rights to freedom of expression and assembly.[289]	
	0 / 2

[286] Galopin and Nelson, 'Live Facial Recognition, (LFR) MPS Legal Mandate', pp. 5–6.

[287] London Policing Ethics Panel, 'Final Report on Live Facial Recognition' (May 2019) <http://www.policingethicspanel.london/uploads/4/4/0/7/44076193/live_facial_recognition_final_report_may_2019.pdf> [accessed 15 July 2022].

[288] Metropolitan Police Service, 'Live Facial Recognition: Legal Mandate'.

[289] Galopin and Nelson, 'Live Facial Recognition, (LFR) MPS Legal Mandate', pp. 5–6.

E.2 Technical reliability

Algorithmic Fairness (Equality Act 2010)	Score
A. Before using FRT, have police evaluated and published the demographic makeup of the training dataset to ensure the dataset is representative of the population where it is to be used?	0 / 1
Notes: The demographic makeup of the training dataset has not been published in MPS' documents. It is likely that this information is not known by MPS due to commercial sensitivity.	
B. Before using FRT, have police evaluated and published FRT's performance across demographic groups, in different conditions that match FRT's operational use, to ensure FRT performs well and similarly across the population?	0 / 1
Notes: There was no published evaluation of LFR's performance before the trial deployments. MPS conducted an internal evaluation but did not disclose the results before or during the LFR deployments. This lack of transparency makes it difficult for outside stakeholders to assess the comprehensiveness of the evaluation and understand whether LFR performs well and similarly across the population. The DPIA states that: 'LFR technologies have been tested under variable operating conditions by both the manufacturer NEO Neoface and the MPS during a series of three trials'.[290] However, the results of this evaluation have not been published. After the deployments, MPS conducted an Equality Impact Assessment (EIA).[291] This EIA frequently refers to an independent evaluation of demographic differences in facial recognition algorithms conducted by the National Institute of Standards and Technology (NIST).[292] NIST evaluates NEC Corporation's algorithm NEC-3. The EIA states that according to the NIST evaluation, NEC 'provided an algorithm for which the false positive differential was undetectable'.[293] However, the application in the NIST evaluation does not match the operational use of LFR. The NIST evaluation was conducted on static, standardised images (e.g. mugshots) rather than moving, wild images which is how LFR is used in practice. In fact, the NIST evaluation notes that they do not address the use of wild images: 'We did not use image data from the Internet nor from video surveillance. This report does not capture demographic differentials that may occur in such photographs'.[294] Further, it is not clear whether MPS uses NEC-3 or a different algorithm developed by NEC.	
	0 / 2

[290] Nelson, 'Metropolitan Police Service Privacy Impact Assessment', p. 11.

[291] Metropolitan Police Service, 'Equality Impact Assessment'.

[292] Grother, Ngan, and Hanaoka, 'Face Recognition Vendor Test'.

[293] Metropolitan Police Service, 'Equality Impact Assessment', p. 13.

[294] Grother, Ngan, and Hanaoka, 'Face Recognition Vendor Test', p. 9.

Robust Practice (Data Protection Act 2018)	Score
C. Are there safeguards precluding the use of FRT with an unsuitable low-quality probe or watchlist image?	0 / 1
Notes: MPS' documents do not indicate any safeguards that preclude the use of LFR with an unsuitable low-quality image. In practice, the poor quality of moving, wild images likely resulted in the high proportion of misidentifications during the LFR deployments, where only 19% of FRT-generated matches yielded verifiably correct matches.	
D. Have police pre-established and met thresholds for the FRT system's accuracy (precision, false positive rate, true positive rate) to inform the legal test of strict necessity for personal data processing?	0 / 1
Notes: There were no pre-established thresholds for the LFR system's precision and true positive rate. The DPIA notes that, 'A technical expert, who has been trained in the use of the equipment, including amending the settings to enhance operating parameters and reduce generation of false positives to below 0.1% will be present at all deployments'.[295] This threshold of 0.1% was not met for one of the LFR deployments (Romford, February 2019, which had a false positive rate of 0.13%). More importantly, there were no pre-established thresholds for other accuracy metrics that are important to inform the legal tests of necessity and proportionality.	
	0 / 2

Deployment Performance (Equality Act 2010)	Score
E. Does FRT perform well (precision, false positive rate, true positive rate) and similarly across demographic groups?	0 / 1
Notes: Across six deployments from June 2018 to February 2019, MPS' use of FRT yielded 8 verifiably correct matches from 42 FRT-generated matches, which means that the precision of FRT matches is 19%.[296] In their report, MPS provides the true positive rates and false positive rates across demographic groups. These results show demographic differentials across gender. For example, the LFR system produced a higher true positive rate for men compared to women.[297] Moreover, MPS did not provide demographic breakdown for the precision of LFR. Given that precision is a critical metric for assessing FRT performance, the incomplete demographic results are concerning.	
	0 / 1

[295] Nelson, 'Metropolitan Police Service Privacy Impact Assessment', p. 15.

[296] Fussey and Murray, *Independent Report*, pp. 69–70.

[297] National Physical Laboratory and Metropolitan Police Service, *Metropolitan Police Service Live Facial Recognition Trials*, p. 26

E.3 Human decision-making

Human Review	Score
A. Is there a transparent evaluation that shows human review of the FRT matches is reliable, given the accuracy of officer-verified matches and the amount of time an officer has to review an FRT match?	0 / 1
Notes: Human review of LFR had a 36% precision, meaning that out of the interventions based on human review of LFR, only 36% of individuals were correctly identified. Across final 6 deployments from June 2018 to February 2019, there were 22 individuals stopped based on LFR matches verified by an officer, and only 8 of these individuals were confirmed to be correctly matched once an identity check took place.[298] This means that the precision of human review was 8/22 = 36%. The University of Essex report on MPS' LFR trial highlights that there were time pressures since the use of LFR was happening in real time.[299] Thus, officers did not have a significant amount of time to review LFR matches, raising concerns about the reliability of human review.	
	0 / 1

Preparation	Score
B. Is training for the particular type of FRT mandated for police officers using the technology?	0 / 1
Notes: Training was not mandated for all officers using LFR during the trial deployments. The DPIA states that a technical expert trained to use LFR was present at all deployments. However, MPS' report notes that, 'Due to the nature of the operational trial deployments, it was not possible to attach the same group of officers to every deployment and provide them with specific training in the adjudication process but such training has been identified as important for future operational deployments'.[300] The adjudication process involves an officer in a control room reviewing the LFR matches and assessing if an intervention should be made, and this indicates that officers were not necessarily trained to use LFR. It is also not clear if street-based officers with mobile devices capable of receiving LFR alerts were trained to use LFR.	
C. Are there clear standards for technical training on using FRT, data protection training, and training on risks including differential treatment, function creep, and unwarranted intrusions?	0 / 1
Notes: The DPIA only indicates technical training for the use of FRT. There are no standards for data protection training and training on the risks of FRT.	
D. Has there been a documented non-operational research trial of FRT with informed consent from participants before the operational use of FRT for policing?	0 / 1
Notes: There has not been a documented non-operational trial of FRT before its operational use. The trials of FRT were operational. The technology was not transparently tested for research purposes before being deployed operationally for policing purposes.	
	0 / 3

[298] Fussey and Murray, *Independent Report*, pp. 69–70.

[299] Fussey and Murray, *Independent Report*, p. 120.

[300] National Physical Laboratory and Metropolitan Police Service, *Metropolitan Police Service Live Facial Recognition Trials*, p. 24.

Accountability	Score
E. Are there clear measures for police to document cases of harm resulting from the use of FRT such as differential treatment, function creep, or unwarranted intrusions?	0 / 1
Notes: There were no clear measures for police to report cases of harm. The University of Essex report on MPS' LFR trial highlights cases of function creep: 'On occasion, individuals were flagged by the LFR technology in relation to a serious offence, but this had already been dealt with by the criminal justice system. However, they were wanted in relation to more minor offences and were arrested accordingly. It is unlikely this lesser offence would have been sufficiently serious to be included in the initial watchlist. This raises additional concerns when LFR is deployed on a necessity calculation intended to address serious crime but is then also used for more minor offences'.[301] Additionally, during one of MPS' trial deployments, a 14-year-old child was stopped and fingerprinted after an FRT misidentification.[302] However, such harms of function creep and unwarranted intrusions were not documented by MPS.	
F. Do police have a whistleblower protection policy to protect persons who reveal FRT misuse?	0 / 1
Notes: MPS does not provide anonymity to whistleblowers.[303] This lack of confidentiality would fail to protect police officers reporting on FRT misuse and might prevent them from reporting cases of misuse. In fact, there have been recent reports of a 'culture of silence' within MPS.[304]	
G. Is there a clear redress mechanism (beyond judicial review and usual complaint procedures) for harmed individuals and groups to participate in an investigation into police use of FRT?	0 / 1
Notes: Based on MPS' documents, there is no clear redress mechanism for those harmed by the use of FRT. MPS' appropriate policy document notes that to meet the accountability principle there is 'a process for ongoing review, both post-Deployment and in relation to the MPS LFR Documents'.[305] However, this does not establish a mechanism for harmed persons to participate in an investigation or review of deployments. This is confirmed by the House of Lords Justice and Home Affairs Committee report on new technologies in the justice system that highlights the lack of recourse for people harmed by the use of technologies such as FRT.[306]	
H. Are there clear measures to ensure that the redress mechanism is procedurally fair?	0 / 1
Notes: There are no clear measures to ensure a procedurally fair redress mechanism; there is no clear redress mechanism for harmed persons in the first place.	
	0 / 4

[301] Fussey and Murray, *Independent Report*, p. 11.

[302] Big Brother Watch, *Briefing on Facial Recognition Surveillance*, p. 16.

[303] Joe Talora, 'No Anonymity for Met Police Whistleblowers, Says Deputy Commissioner Sir Stephen House', *Evening Standard* (17 November 2021) <https://www.standard.co.uk/news/london/met-police-misconduct-no-anonymity-whistleblowers-deputy-commissioner-stephen-house-b966743.html> [accessed 15 July 2022].

[304] Joe Talora, 'Met Police Whistleblowers Need Anonymity to Tackle "Culture of Silence", Says Top London Tory' (3 February 2022) <https://www.standard.co.uk/news/london/metropolitan-police-cressida-dick-misconduct-iopc-london-tory-susan-hall-b980408.html> [accessed 15 July 2022].

[305] Metropolitan Police Service, 'Appropriate Policy Document for Sensitive Data Processing Within Live Facial Recognition Deployments', p. 6.

[306] House of Lords, Justice and Home Affairs Committee, Technology Rules?, p. 37.

E.4 Expertise and oversight

Ethics Committee	Score
A. Is regular oversight from an ethics committee mandated throughout the life of the FRT project?	0 / 1
Notes: There was a lack of oversight throughout the life of the FRT project from the concept stage. The London Policing Ethics Panel (LPEP) is an ethics committee that oversees the way London is policed. Even though the panel was in place from 2014, the panel only started providing oversight in early 2018 after MPS was already using FRT, based on the published meeting minutes.[307]	
B. Are there clear processes for the committee to influence if and how FRT is implemented, including the power of veto for the FRT project?	0 / 1
Notes: The London Policing Ethics Panel (LPEP) is advisory and does not have the power of veto for the FRT project. The LPEP Terms of Reference note that, 'There is a presumption (not a requirement) that recommendations of the Panel will be acted upon (but an understanding that some may be operationally or financially challenging). In all cases the recommendations will be responded to by the Commissioner within a specified period'.[308] We note that MPS did consider and implement a number of the Panel's recommendations outlined in the Panel's July 2018 interim report and May 2019 final report on the use of LFR. However, MPS was not required to act upon the Panel's recommendations, and the Panel itself does not have decision-making power to influence if and how LFR is implemented.	
C. Is the committee an independent body from police organisations with members having non-policing backgrounds and with safeguards to ensure the committee's sustainability even without political support?	0 / 1
Notes: The London Policing Ethics Panel (LPEP) partially satisfies this question, as the panel is an independent body set up by the Mayor of London.However, there is no requirement for members to have a non-policing background, and there is a lack of transparent safeguards to ensure the committee's sustainability. The LPEP Terms of Reference note that, 'Members of the Panel (and their close relatives) may not have a past or current connection with MOPAC and/or the MPS which could be seen to affect their independence'.[309] However, members of the panel can still have a policing background, for example, with another police force in the UK. We note that during the time of the LFR trial, the panel only included members with non-policing backgrounds.[310] However, currently LPEP has members with a background in police service, including a member who served as an officer with the MPS. This is concerning given the requirement of the Terms of Reference. Additionally, the Terms of Reference does not outline any safeguards to ensure the committee's sustainability.	

[307] London Policing Ethics Panel, 'Minutes of Meeting, 12 February 2018' <http://www.policingethicspanel.london/uploads/4/4/0/7/44076193/lpep_minutes_12_february_2018.pdf> [accessed 15 July 2022].

[308] Mayor of London, Mayor's Office for Policing and Crime, 'London Policing Ethics Panel Terms of Reference' <http://www.policingethicspanel.london/uploads/4/4/0/7/44076193/london_policing_ethics_panel_terms_of_reference_2017.pdf> [accessed 15 July 2022].

[309] Mayor of London, Mayor's Office for Policing and Crime, 'London Policing Ethics Panel Terms of Reference'.

[310] London Policing Ethics Panel, 'Final Report on Live Facial Recognition'.

Ethics Committee (continued)	Score
D. Is the committee diverse in terms of demographic makeup and independent expertise in human rights, equality, and data protection?	0 / 1
Notes: The London Policing Ethics Panel (LPEP) had an unknown demographic diversity and lacked human rights, data protection, and equality experts. The panel's final report on LFR lists the panel members during the time of the trial.[311] The demographic diversity of the panel has not been published. The LPEP Terms of Reference also do not mention any consideration of demographic diversity for the selection of members.[312] During their evaluation of the MPS' trial, LPEP engaged with civil society organisations and external experts. However, the panel itself lacked experts in human rights, data protection, and equality. The Terms of Reference also do not indicate that expertise from these areas is required or recommended.	
E. Are detailed meeting minutes published, including briefing papers, discussions, and conclusions?	0 / 1
Notes: Detailed meeting minutes are not published. The London Policing Panel's published minutes are brief. For the LFR project, briefing papers and details of discussions are not made public. We acknowledge that the panel did publish an interim report and final report on MPS' use of FRT.[313] These reports included recommendations, and MPS publicly responded to the final report.[314] However, the panel's deliberations throughout the trials are not published. For example, during the February 2018 meeting, the Surveillance Camera Commissioner and Information Commissioner joined to discuss issues around police use of new technology, including FRT. The meeting minutes briefly state, 'The discussion included the powers that the Commissioners did and did not have in this sphere, the regulatory environment and their views of the key issues'.[315] However, the details of the discussion are not included. Other meetings that discuss FRT similarly do not provide the details of discussions.[316]	
	0 / 5

[311] London Policing Ethics Panel, 'Final Report on Live Facial Recognition'.

[312] Mayor of London, Mayor's Office for Policing and Crime, 'London Policing Ethics Panel Terms of Reference'.

[313] London Policing Ethics Panel, 'Interim Report on Live Facial Recognition' (July 2018) <http://www.policingethicspanel.london/uploads/4/4/0/7/44076193/lpep_report_-_live_facial_recognition.pdf> [accessed 15 July 2022]; London Policing Ethics Panel, 'Final Report'.

[314] Ephgrave, 'MPS Response to the London Policing Ethics Panel'.

[315] London Policing Ethics Panel, 'Minutes of Meeting, 12 February 2018', p. 1.

[316] London Policing Ethics Panel, 'Minutes of Meeting, 9 July 2018' <http://www.policingethicspanel.london/uploads/4/4/0/7/44076193/lpep_minutes_9_july_2018.pdf> [accessed 15 July 2022]; London Policing Ethics Panel, 'Minutes of Meeting, 11 June 2018' <http://www.policingethicspanel.london/uploads/4/4/0/7/44076193/2018_06_11_lpep_minutes_11_june_2018.pdf> [accessed 15 July 2022]; London Policing Ethics Panel, 'Minutes of Meeting, 14 May 2018' <http://www.policingethicspanel.london/uploads/4/4/0/7/44076193/2018_05_14_lpep_minutes_14_may_2018.pdf> [accessed 15 July 2022].

Civil Society and Experts	Score
F. Are there transparent, proactive consultations with civil society and independent experts on the particular type of FRT?	0 / 1
Notes: MPS provides a consultation log in their most recent EIA developed after the FRT trials.[317] The EIA indicates a lack of proactive consultations with civil society and independent experts. According to the consultation log, MPS only consulted with the Ada Lovelace Institute (ALI), experts at Essex University, and MPS Independent Advisory Groups in 2019. These consultations started a significant period of time after the use of FRT in 2016. The consultation with ALI also lacks transparency; it is not clear what recommendations ALI provided to the MPS. We also observe that most of MPS' consultations are with police associations or police service organisations. MPS' report on the FRT trials notes that, 'Prior to the first trial at Notting Hill Carnival, the MPS sought the views of community groups and the civil liberty group, Big Brother Watch'.[318] However, there is a lack of transparency about the engagement, especially with regard to the outcomes and the stage of the FRT project at which views were sought. Such transparency is crucial, especially given contradicting information in the University of Essex evaluation that engagements with civil society groups were responsive rather than proactive.[319]	
G. Are police required to consider the advice from consultations and transparently explain the outcomes, including providing a justification if the advice is not followed?	0 / 1
Notes: MPS is not required to consider the advice from consultations. While MPS briefly explains the outcome of consultations in their consultation log, it is not specifically articulated how the advice was taken into account and justified if the advice was not followed. For example, for the MPS' consultation with the Ada Lovelace Institute (ALI), the EIA writes that, 'The MPS has actively engaged with ALI and considered their recommendations in line with their 3 key Aims. MPS were invited to attend ALI forum meetings to increase LFR understanding and transparency'.[320]	
	0 / 2

[317] Metropolitan Police Service, 'Equality Impact Assessment'.

[318] National Physical Laboratory and Metropolitan Police Service, *Metropolitan Police Service Live Facial Recognition Trials*, p. 7.

[319] Fussey and Murray, *Independent Report*, p. 63.

[320] Metropolitan Police Service, 'Equality Impact Assessment', p. 25.

Community Engagement	Score
H. Are there clear, proactive processes for the public, especially marginalised communities, to influence if and how FRT is implemented?	0 / 1
Notes: There were no clear, proactive processes for the public, especially marginalised communities, to influence if and how FRT was implemented. Some concerns: (a) MPS' data protection impact assessment (DPIA) states that: 'All deployments will be in public spaces and will be overt and may be signposted, a consideration which will be decided upon by the Command team, who will take account of the aims and objectives of the operation. This will be in accordance with MPS signs with clear statements; Police Operation – Cameras in Use. It will be further supported by leaflets which will provide information on the operation and a link inviting members of the public to share their views and complete a survey as part of the consultation process'.[321] These engagements with the public were during the FRT trials, and there is no indication of consultations with the public before the FRT trials. (b) It is also not clear whether the survey enabled the public to influence how and whether FRT was implemented. (c) MPS' first Community Impact Assessment (CIA) on LFR, which was created in February 2020, suggests that the earliest consultations with community representatives were in 2019 after the trial deployments.[322] (d) The CIA states that: 'The London representatives for the LGBT IAG and the Race IAG were both consulted in October 2019'.[323] However, there are no further details about the outcome of this consultation. It is not clear if and how these representatives were able to influence the implementation of FRT.	
I. Are all FRT materials accessible to people with disabilities and provided in immigrant languages?	0 / 1
Notes: MPS' documents on LFR may not be accessible to people with disabilities, and the documents are not provided in immigrant languages. As of the audit evaluation date (July 2022), the MPS website is not fully compliant with accessibility regulations: 'This website is partially compliant with the Web Content Accessibility Guidelines version 2.1 AA standard, due to the non-compliances listed below [...] PDFs may not be suitable for users of assistive technology. We are in the process of replacing or fixing any PDF and Word documents which are essential to our services, however users can request accessible versions'.[324] It is not clear whether requesting accessible versions was an option during the time of the LFR trials that ran from 2016 to 2019. These accessibility issues can pose barriers to certain communities and make it difficult to understand the use and impact of LFR.	
	0 / 2

[321] Nelson, 'Metropolitan Police Service Privacy Impact Assessment', p. 3.

[322] Metropolitan Police Service, 'Community Impact Assessment: Op Fahrenheit – MPS Live Facial Recognition' (11 February 2020) <https://www.met.police.uk/SysSiteAssets/foi-media/metropolitan-police/disclosure_2020/august_2020/live-facial-recognition-technology-att2.pdf> [accessed 15 July 2022].

[323] Metropolitan Police Service, 'Community Impact Assessment', p. 2.

[324] Metropolitan Police Service, 'Accessibility' <https://www.met.police.uk/hyg/accessibility/> [accessed 17 July 2022].

F. South Wales Police's Trial of Mobile Phone Facial Recognition

Police Force: South Wales Police (SWP)

Facial Recognition Type: Mobile Phone or Operator Initiated Facial Recognition (OIFR)

OIFR Deployment Dates: Trial deployments from December 2021 to March 2022

Audit Evaluation Date: July 2022

Key Resources Used: **SWP Documents**, **SWP EIA**, **SWP Deployment Results**

Our final case study is of the recent operational trial of mobile phone or operator initiated facial recognition (OIFR) conducted by South Wales Police (SWP) from December 2021 to March 2022.[325] SWP provided more documentation about their use of OIFR in comparison with their trial of live facial recognition, which was ruled unlawful in the *Bridges* court case. Although there were improvements, significant gaps remain with regard to the minimum legal and ethical standards. We highlight the lack of (a) limited criteria for who is included in the watchlist, (b) full transparency for evaluations of discrimination, and (c) independent oversight and community engagement.

First, the watchlist included all custody images of South Wales Police with no limits on the seriousness of offence.[326] This broad inclusion raises concerns about the legal requirements of necessity and proportionality, especially whether distinct necessity tests for each category of individuals on the watchlist were conducted. Moreover, the watchlist included the images of innocent persons who were arrested but not convicted, even though these images are unlawful to retain.[327]

Second, while SWP took proactive steps to evaluate bias and discrimination, there was a lack of full transparency for these evaluations. SWP evaluated OIFR's accuracy before its operational use and found no evidence of algorithmic bias. However, SWP did not publish the demographic distribution of the evaluation dataset, which is crucial to assess bias. Additionally, SWP provided the demographic data for the people on which OIFR was used, but the demographic data for the watchlist and those arrested remain unknown.

Finally, there were notable gaps in oversight and community engagement. SWP engaged with the SWP Joint Independent Ethics Committee before and after the OIFR trial. However, the committee consists of police officers and is a body situated within the police, raising concerns about the independence of the oversight. Based on the most recently published meeting minutes, there were no independent experts in human rights, equality, or data protection on the committee. Moreover, SWP did not conduct consultations with the public, nor with civil society, to gather feedback before or during the OIFR trial.

[325] In December 2021, Gwent Police reported that they would be trialling OIFR alongside South Wales Police using the same policies. However, in April 2022, Gwent Police responded to a freedom of information request stating that, 'We can confirm that the Operator Initiated Facial Recognition app is not used within Gwent Police due to technical issues.' There is no transparency about the details of these technical issues. See Gwent Police, 'Response to Freedom of Information Request 2022/25016'.

[326] Custody images are photographs taken by police when an individual is arrested.

[327] South Wales Police considers the deletion of unconvicted custody images upon request and is actively working to find a solution to automatically remove these images. However, currently unconvicted custody images are still included in the watchlist by default, even though they are unlawful to retain. *See RMC and FJ v. Commissioner of Police for the Metropolis and Secretary of State for the Home Department.*

Below we provide the full audit scorecard for this case study, which includes the score and accompanying explanation for each question.

F.1 Legal standards

In Accordance with the Law (Human Rights Act 1998)	Score
A. Are there clear, objective, and limited criteria for who can be included in the watchlist, including with regard to the image source and the seriousness of offence or risk?	0 / 1
Notes: The criteria for who can be included in the watchlist are not limited with regard to the seriousness of offence or risk. The SWP Policy document indicates that OIFR used (a) South Wales Police and Gwent Police custody images and (b) South Wales Police images of missing persons.[328] These criteria are clear and objective. There are limits with regard to the image source, as the watchlists are 'a direct duplication of the images that are currently legitimately stored in Niche RMS, which is the source of custody and missing person images' as noted in SWP's data protection impact assessment (DPIA).[329] However, the criteria are still broad given that there are no limits with regard to the type of offence or risk.	
B. Are there clear, objective, and limited criteria for where and when FRT can be used, including mandating reasonable suspicion that persons on the watchlist will be at the location and requiring a high grade of intelligence for the police intelligence case that supports FRT use?	0 / 1
Notes: We highlight a few concerns with regard to the criteria for where and when OIFR can be used. (1) There are limits for when OIFR can be used, but some of the criteria lack clarity and potentially leave broad discretion to individual police officers. According to Standard Operating Procedure, grounds for using OIFR include: 'Is suspected to be: a. Of having committed a criminal offence or is unlawfully at large with further police action required. b. Subject of bail conditions, court order or other restriction that would be breached if they were at the location at the time. c. Missing persons deemed increased risk. d. Presenting a risk of harm to themselves or others. e. Subject is deceased or it has been confirmed that they are deceased'.[330] It is unclear, for example, how an individual would be suspected of being a subject of bail conditions or a court order. (2) There are no clear limits for the locations where OIFR can be used, and OIFR can presumably be used at any location. (3) There is no indication of a threshold of suspicion for the grounds of use. There is also no indication of a threshold of intelligence for 'the case supporting the prospects of identifying a person' as described in the Standard Operating Procedure.[331]	
C. Are there clear, objective, and limited criteria concerning third-party access to the data collected or retained, including with regard to what data can be shared, with whom it can be shared, and for what specific purpose it can be shared?	0 / 1
Notes: There are broad criteria concerning access to the data collected or retained. There are no clear limits regarding what information can be shared and the specific reason for which information can be shared. SWP's DPIA states that, 'Information will only be shared where necessary for a policing purpose on a case-by-case basis therefore no agreement is necessary. A contract will be in place with the algorithm supplier. Information could be shared with Home Office Biometrics, the Defence Science and Technology Laboratory and academic partners as part of the wider academic evaluation over the proof-of-concept matters within the project. However, this could only be facilitated using available information captured within the defined retention periods'.[332]	
	0 / 3

[328] South Wales Police and Gwent Police, 'Policy Document for the Overt Use of Operator Initiated Facial Recognition (OIFR)' (25 January 2022) <https://www.south-wales.police.uk/SysSiteAssets/media/downloads/south-wales/about-us/frt/oifr-documents/oifr-policy-v0.4.pdf> [accessed 17 July 2022], p. 21.

[329] South Wales Police and Gwent Police, 'Data Protection Impact Assessment for Operator Initiated Facial Recognition (OIFR)' <https://www.south-wales.police.uk/SysSiteAssets/media/downloads/south-wales/about-us/frt/oifr-documents/oifr-dpia-v0.5.pdf> [accessed 15 July 2022], p. 8.

[330] South Wales Police and Gwent Police, 'Standard Operating Procedures for the Overt Use of Operator Initiated Facial Recognition (OIFR)' (25 January 2022) <https://www.south-wales.police.uk/SysSiteAssets/media/downloads/south-wales/about-us/frt/oifr-documents/oifr-sop-v0.6.pdf> [accessed 17 July 2022], p. 4.

[331] South Wales Police and Gwent Police, 'Standard Operating Procedures for the Overt Use of Operator Initiated Facial Recognition (OIFR)', p. 5.

[332] South Wales Police and Gwent Police, 'Data Protection Impact Assessment for Operator Initiated Facial Recognition (OIFR)', p. 32.

Necessary in a Democratic Society (Human Rights Act 1998)	Score
D. Have police identified less intrusive alternative measures and proven that FRT is strictly necessary compared to these measures using scientifically verifiable evidence?	0 / 1
Notes: There is no published necessity analysis that proves that FRT is strictly necessary compared to less intrusive alternative measures using scientifically verifiable evidence. With regard to the 'necessary in a democratic society' test, SWP's Legal Mandate articulates that: 'The use of OIFR should be considered against other methods of identifying persons of interest to SWP/GWP and/or UK Law Enforcement. Consideration should be given as to the effectiveness and intrusiveness of other viable methods that could give the same result, with the least intrusive, viable method being adopted to progress an investigation'.[333] The Legal Mandate then provides an example: 'The use of OIFR to confirm or eliminate a person's identity may be less intrusive to arresting the individual in order to later confirm their identity at a police station using fingerprints or DNA'.[334] However, SWP does not provide any scientifically verifiable evidence to support this claim, and it is not clear why FRT is strictly necessary compared to identifying individuals at a police station using fingerprints or DNA. There is also no evidenced comparison of FRT with any other alternative measures.	
E. Have police conducted distinct necessity tests with an evidence-based justification for each category of individuals on the watchlist?	0 / 1
Notes: SWP's Legal Mandate does not include distinct necessity tests with an evidence-based justification for each category of individuals on the watchlist. We highlight a couple of key concerns: (1) The Legal Mandate provides an example analysis for the case where OIFR is used 'to find vulnerable individuals who are missing and believed to be at risk of child sexual abuse' but the analysis is inadequate and lacks an evidence-based justification.[335] The analysis compares using OIFR with using public appeals: 'At times, the police may also enlist the public to help with locating missing people through the use of public appeals, by circulating a photograph of a vulnerable child across the media. This is a potentially much greater intrusion to the individual's privacy rights given the aim of the public appeal is for wide-scale awareness and that information goes outside of police control when it is placed in the public domain. Where it might be viable to use OIFR as a tool for identification instead, the intrusion on the individual's privacy rights can be lower, yet it still offers SWP/GWP a route to discharge its common law responsibilities to protect life'.[336] This analysis does not consider the intrusion to the privacy rights of people on which OIFR is used who are not the missing individual. There is also no scientifically verifiable evidence provided in the justification. (2) There is no evidence-based necessity analysis for other categories of individuals on the watchlist. For example, it is not clear how the seriousness of the offence informs SWP's necessity analysis and why the images of people who have committed minor offences are strictly necessary to be included in the watchlist.	

[333] South Wales Police and Gwent Police, 'Operator Initiated Facial Recognition (OIFR) Legal Mandate' (25 January 2022) <https://www.south-wales.police.uk/SysSiteAssets/media/downloads/south-wales/about-us/frt/oifr-documents/oifr-legal-mandate-v0.4.pdf> [accessed 15 July 2022], p. 8.

[334] South Wales Police and Gwent Police, 'Operator Initiated Facial Recognition (OIFR) Legal Mandate', p. 8.

[335] South Wales Police and Gwent Police, 'Operator Initiated Facial Recognition (OIFR) Legal Mandate', p. 7.

[336] South Wales Police and Gwent Police, 'Operator Initiated Facial Recognition (OIFR) Legal Mandate', p. 7-8.

Necessary in a Democratic Society (Human Rights Act 1998) (continued)	Score
F. Have police shown that FRT does not disproportionately limit the human rights of affected persons, including those who are misidentified, not on the watchlist, or impacted by unwarranted intrusions?	0 / 1
Notes: SWP does not adequately assess whether OIFR disproportionately limits the human rights of those misidentified, not on the watchlist, or impacted by unwarranted intrusions. We highlight some key concerns: (1) With regard to proportionality, SWP’s Legal Mandate states that ‘OIFR cannot be used to identify persons unless they have been included on [a watchlist][337]’. However, there remains the possibility that OIFR misidentifies an individual who is not on the watchlist, and the impact on those misidentified is not adequately assessed. (2) SWP’s data protection impact assessment states that: ‘If the Probe Image is incorrectly matched against a Candidate Image this may result in an unlawful arrest. The risk here is no more prevalent than in current police practices when integrating police indices'.[338] However, SWP does not show that risk is no more prevalent than in current police practice. For example, there is no evidence that the misidentification rate with OIFR matches that of police officers. Further, the scope of OIFR is different and broader than current police practice, given that OIFR enables police to identify an individual against all custody images without arresting them and detaining them at a police station. (3) It is concerning that SWP’s equality impact assessment regards facial recognition as a ‘Non-Invasive Identity Verification'.[339] This indicates a likely inadequate proportionality analysis that does not consider OIFR’s invasiveness and impact on the human rights of affected persons.	
	0 / 3

[337] South Wales Police and Gwent Police, ‘Operator Initiated Facial Recognition (OIFR) Legal Mandate’, p. 8.

[338] South Wales Police and Gwent Police, ‘Data Protection Impact Assessment for Operator Initiated Facial Recognition (OIFR)’, p. 37.

[339] South Wales Police, ‘Equality Impact Assessment: Facial Recognition Technology – Retrospective, Live and Operator Initiated’, p. 4.

Data Protection (Data Protection Act 2018)	Score
G. Before using FRT, have police carried out and published a data protection impact assessment and appropriate policy document for sensitive data processing?	0 / 1
Notes: SWP carried out a data protection impact assessment (DPIA) and appropriate policy document before using OIFR, but the DPIA was only published after the OIFR trial started. The OIFR trial started in December 2021 and ended in March 2022. However, the DPIA was published in early 2022 almost two months after SWP announced on 7 December 2021 that they would be trialling OIFR[340] — the DPIA and standard operating procedures document were only signed off on 25 January 2022. Publishing documents after the start of a trial makes it difficult for the public and outside stakeholders to understand, scrutinise, and share feedback before the technology is used operationally.	
H. Beyond social media or website publishing, have police used other means to inform potential data subjects or most people in their jurisdiction in advance about when, where, why, and how FRT is being used and how they can exercise their individual rights?	0 / 1
Notes: Beyond social media and website publishing, SWP did not use other means to inform people in advance about the use of OIFR. The OIFR Policy document notes that, 'In advance of OIFR pilot ensure that: – a) The OIFR pilot is notified to the public using SWP/GWP website and other appropriate communication channels (including social media); and b) literature is prepared for Subjects (to include information outlined within a privacy notice)'.[341] SWP announced their deployment in a news article and in a Twitter post in December 2021; SWP also published documents about OIFR use in early 2022 on their website.[342] These communication efforts to inform people were limited to social media and website publishing. They also do not clearly indicate the locations where OIFR is used. Additionally, the documents about OIFR use were not published in advance of the OIFR trial which started in December 2021.	
I. Are there clear measures to ensure data subjects can exercise their individual rights including the rights to rectification, erasure, and object with clear justifications if exemptions apply?	0 / 1
Notes: SWP's DPIA and Privacy Notice indicate how some individual rights such as the right of access can be exercised. However, the DPIA and Privacy Notice do not clearly articulate whether and how data subjects can exercise their right to object. In reference to the right to object, the DPIA only states, 'Each use of OIFR will have a compelling, legitimate grounds [sic] which are documented beforehand'.[343] The Privacy Notice states that, 'You have the right to object to: processing based on legitimate interests or performance of a task in the public interest and or exercise of official authority'.[344] The OIFR Policy document articulates that, 'there is no power to require an individual's cooperation in having their image captured'.[345] However, there are no clear measures to ensure that individuals can easily refuse to cooperate in having their image captured. Additionally, for the rights to erasure and rectification, there is no indication of a policy for recording requests for erasure and rectification that are made in person. This is crucial given that individuals stopped and scanned using OIFR may likely make requests in person. The ICO highlights the importance of 'a policy for recording details of the requests you receive, including those made by telephone or in person' for compliance.[346]	

[340] South Wales Police, 'New Facial Recognition Mobile App'.

[341] South Wales Police and Gwent Police, 'Policy Document for the Overt Use of Operator Initiated Facial Recognition (OIFR)', p. 19.

[342] South Wales Police, 'New Facial Recognition Mobile App'; South Wales Police Twitter Account, @swpolice, tweet (8 December 2021): '#NEWS | Alongside @gwentpolice, we have developed the first mobile app for Facial Recognition in UK policing. It will be trialled over the next three months. [film camera emoji]Here, @ACCMarkTravis explains more about how Facial Recognition Technology and the new mobile app will be used.'

[343] South Wales Police and Gwent Police, 'Data Protection Impact Assessment for Operator Initiated Facial Recognition (OIFR)', p. 24.

[344] South Wales Police, 'Privacy Notice' <https://www.south-wales.police.uk/hyg/southwales/privacy-notice/> [accessed 17 July 2022].

[345] South Wales Police and Gwent Police, 'Policy Document for the Overt Use of Operator Initiated Facial Recognition (OIFR)', p. 19.

[346] Information Commissioner's Office, 'The Right to Rectification' <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-le-processing/individual-rights/the-right-to-rectification/> [accessed 15 July 2022]'.

Data Protection (Data Protection Act 2018) (continued)	Score
J. Do police check the watchlist against the data source close to the time of deployment to ensure the watchlist is accurate and up to date?	1 / 1
Notes: SWP checks the watchlist against the Niche RMS source system close to the time of the deployment to ensure the watchlist is accurate and up to date. The DPIA notes that, 'Data will be checked against source SWP/GWP databases, managed in accordance with MOPI standards. These databases are kept up to date as required for effective law enforcement so that personal data which is known to be inaccurate, materially incomplete or no longer up to date is not transmitted. The core source database is Niche RMS which undergoes rigorous checks and balances to ensure the data is accurate and fit for purpose'.[347] The DPIA provides further details about how watchlist images are kept up to date with the source system: 'Currently there are circa 760k images in the SWP /GWP Niche RMS source system, all images will be bulk uploaded to the Image Reference Database upon pilot go-live with additional custody images added from the source system ten minutes after image capture in the source system. Missing person images are updated in the Image Reference Database every hour. This will involve both new images being added and any images which are no longer flagged as missing persons in the source system are also un-enrolled from the Image Reference Database'.[348]	
K. Are there clear measures to ensure that watchlist images are lawfully held, have a known provenance, and exclude unconvicted custody images?	0 / 1
Notes: The watchlist does not exclude unconvicted custody images, even though these images are unlawful to retain.[349] Although SWP considers the deletion of unconvicted custody images upon request and is working towards a solution to remove them, unconvicted custody images can still be included in the watchlist. This raises concerns about innocent people being identified and facing intrusive interventions with the use of OIFR. The DPIA indicates that the watchlist 'must only contain images lawfully held by police with consideration also being given as to: the legal basis under which the image has been acquired; and the source of the image, particularly where the image is derived from a sensitive or third-party source and may risk compromising that source or exposing that source to risk'.[350] However, with regard to non-convicted custody images, the DPIA writes that, 'Upon go live for the FRT System a script has been run against Niche RMS to bulk enrol the custody images into the FRT System. Consideration has been given to automatically removing images of un-convicted persons but at this stage it is not possible due to the technical legacy build of the system […] At present due to the size of the task to apply automatic deletion it has not been deemed proportionate to manually remove non-convicted custody images from the Image Reference Database as this will negate the benefits of using the technology'.[351] At the same time, the DPIA notes that, 'SWP/GWP are actively engaged with the Niche RMS supplier to develop automated deletion of non-convicted custody images'.[352]	

[347] South Wales Police and Gwent Police, 'Data Protection Impact Assessment for Operator Initiated Facial Recognition (OIFR)', p. 25.

[348] South Wales Police and Gwent Police, 'Data Protection Impact Assessment for Operator Initiated Facial Recognition (OIFR)', p. 13.

[349] *RMC and FJ v. Commissioner of Police for the Metropolis and Secretary of State for the Home Department*.

[350] South Wales Police and Gwent Police, 'Data Protection Impact Assessment for Operator Initiated Facial Recognition (OIFR)', p. 10.

[351] South Wales Police and Gwent Police, 'Data Protection Impact Assessment for Operator Initiated Facial Recognition (OIFR)', pp. 9–10.

[352] South Wales Police and Gwent Police, 'Data Protection Impact Assessment for Operator Initiated Facial Recognition (OIFR)', p. 38.

Data Protection (Data Protection Act 2018) (continued)	Score
L. Via direct consultation, have police proactively considered views of the public, especially marginalised communities, on the particular type of FRT and justified a disregard of the views if relevant?	0 / 1
Notes: SWP did not directly and proactively consult the public on their views on OIFR. In the DPIA, SWP cites surveys conducted to gather views on the use of LFR, but SWP does not consider public views specifically on the use of OIFR. Further, when considering survey results on LFR, SWP does not consider results on the views of marginalised groups, who may be most affected by the technology.	
M. Have police published their procurement contracts and data-sharing agreements with other parties?	0 / 1
Notes: While the DPIA provides some details about information-sharing agreements, these agreements are not published and available for public scrutiny. The DPIA states that a vendor contract will be in place and that an information-sharing agreement will exist with academic evaluators. However, these documents are not published. The DPIA also notes that, 'Information will only be shared where necessary for a policing purpose on a case-by-case basis therefore no agreement is necessary […] Information could be shared with Home Office Biometrics […] as part of the wider academic evaluation over the proof-of-concept matters within the project. However, this could only be facilitated using available information captured within the defined retention periods'.[353] The lack of an agreement and clear restrictions on data sharing between SWP and the Home Office raises the concern that OIFR could be used to identify and deport undocumented migrants, a risk identified by the Joint Council for the Welfare of Immigrants.	
	1 / 7

[353] South Wales Police and Gwent Police, 'Data Protection Impact Assessment for Operator Initiated Facial Recognition (OIFR)', p. 32.

Non-Discrimination (Human Rights Act 1998 and Equality Act 2010)	Score
N. Before using FRT, have police carried out and published an equality impact assessment?	0 / 1
Notes: SWP carried out an equality impact assessment (EIA) before using OIFR but did not publish the assessment prior to the OIFR trial. The OIFR trial started in December 2021 and ended in March 2022. As of the audit evaluation date (July 2022), the EIA still has not been published on the SWP website, although we obtained a copy of the EIA via email in June 2022 under a Freedom of Information request.	
O. For each deployment, have police published the demographic makeup of the watchlist?	0 / 1
Notes: The demographic makeup of the watchlist has not been published in SWP's documents on their use of OIFR. SWP only indicates in the DPIA that the size of the watchlist is approximately 760k images.[354]	
P. For each deployment, have police published the demographic makeup of the population where FRT is used?	1 / 1
Notes: SWP's equality impact assessment includes the demographic makeup of the persons on which OIFR was used. (1) With regard to ethnicity: 'There were 4 uses with Arabic North African subjects. There were 4 uses recorded with Asian subjects (but this was one subject duplicated who was deceased at the morgue.) There were 4 uses recorded with Black subjects, (However two of these people are the same subject and BWV clearly shows the subject to be Asian.) There were 2 uses with White Southern European subjects. There were 25 uses with White Northern European subjects. There were 3 uses recorded as Ethnicity unknown. (Matched data shows 1 Asian, 1 White NE, 1 previously listed on Niche as Asian/White/Arabic NA and Unknown)'.[355] (2) With regard to gender: '39 photographs obtained were of Male subjects. 3 were obtained of females'.[356] (3) With regard to age: '10 – 17, recorded uses 6 with 3 subjects. 18 – 30, recorded uses 21 with 20 subjects. 31 – 60, recorded uses 15 with 12 subjects'.[357]	
Q. For each deployment, have police published the demographic data for arrests, stop and searches, and other outcomes resulting from the use of FRT?	0 / 1
Notes: The demographic data across outcomes are not published. In the equality impact assessment, SWP includes the demographic makeup of the persons on which OIFR was used but does not include the demographic data for the reported outcomes: 11 arrests in total were made, 4 persons were reported for summons for offences, and Safeguarding measures were used in 5 cases.[358]	
	1 / 4

[354] South Wales Police and Gwent Police, 'Data Protection Impact Assessment for Operator Initiated Facial Recognition (OIFR)', p. 12.

[355] South Wales Police, 'Equality Impact Assessment: Facial Recognition Technology – Retrospective, Live and Operator Initiated', pp. 21–22.

[356] South Wales Police, 'Equality Impact Assessment: Facial Recognition Technology – Retrospective, Live and Operator Initiated', p. 21.

[357] South Wales Police, 'Equality Impact Assessment: Facial Recognition Technology – Retrospective, Live and Operator Initiated', p. 22.

[358] South Wales Police, 'Facial Recognition App Pilot Results'.

Free Expression and Assembly (Human Rights Act 1998)	Score
R. Have police assessed FRT's potential 'chilling effect' on the rights to freedom of expression and assembly to inform the legal test of 'necessary in a democratic society'?	0 / 1
Notes: While SWP identifies the risk of OIFR limiting the rights to freedom of expression and assembly in the Legal Mandate, there is no analysis of OIFR's potential chilling effect on these rights. The SWP Legal Mandate notes that: 'In deciding the use of OIFR is necessary and proportionate, regard should be had to an individual's Article 10 and 11 rights – noting there may be expectations of anonymity in a crowd and that individuals may choose to alter their means of demonstration as a result of OIFR use'.[360] However, there is no assessment of the extent to which OIFR may shift people's behaviour and cause a chilling effect on fundamental rights.	
S. Do police preclude using FRT to identify those peacefully participating in an assembly?	0 / 1
Notes: SWP does not preclude using OIFR to identify those peacefully participating in an assembly. In the DPIA, SWP responds to the risk to the rights to freedom of expression and assembly by stating that, 'The assessment prior to any use of OIFR will determine whether interference with these rights is necessary, proportionate and lawful and whether there are less intrusive methods which could be employed. Full, robust justification will be documented during use'.[361] However, SWP does not pre-establish any restrictions on the use of OIFR at assemblies.	
	0 / 2

[360] South Wales Police and Gwent Police, 'Operator Initiated Facial Recognition (OIFR) Legal Mandate', p. 10.

[361] South Wales Police and Gwent Police, 'Data Protection Impact Assessment for Operator Initiated Facial Recognition (OIFR)', p. 37.

F.2 Technical reliability

Algorithmic Fairness (Equality Act 2010)	Score
A. Before using FRT, have police evaluated and published the demographic makeup of the training dataset to ensure the dataset is representative of the population where it is to be used?	0 / 1
Notes: The demographic makeup of the training dataset has not been published in SWP's documents. It is likely that this information is not known by SWP due to commercial sensitivity.	
B. Before using FRT, have police evaluated and published FRT's performance across demographic groups, in different conditions that match FRT's operational use, to ensure FRT performs well and similarly across the population?	0 / 1
Notes: Although SWP conducted an evaluation of OIFR's performance, the results were not published before the use of OIFR, and the results do not indicate the demographic distribution of the evaluation dataset, which is crucial to assess if FRT performs similarly across the population. SWP conducted an internal evaluation of OIFR's performance before using the technology operationally. The EIA reports the results of this evaluation: 'On every occasion the image searched within app returned a match for the subject, regardless of Ethnicity, Gender, or age and ranked the subject as the number one result without exception'.[362] Although these evaluation results indicate that OIFR performs well, the results of the evaluation were not published before the OIFR trial, raising concerns about transparency with the public. Further, the demographic distribution of the evaluation dataset has not been published. It is critical for the evaluation dataset to be demographically diverse to ensure that OIFR performs similarly across the population.	
	0 / 2

[362] South Wales Police, 'Equality Impact Assessment: Facial Recognition Technology – Retrospective, Live and Operator Initiated', p. 21.

Robust Practice (Data Protection Act 2018)	Score
C. Are there safeguards precluding the use of FRT with an unsuitable low-quality probe or watchlist image?	0 / 1
Notes: Although there are safeguards for watchlist images, OIFR can still be used with an unsuitable low-quality probe image, which could result in a misidentification. The Legal Mandate notes that for adding an update to the watchlist, the OIFR system 'will assess the image for quality and suitability for matching in order to allow SWP/GWP personnel to consider and manage the risk of poor quality images generating inaccurate OIFR returns'.[363] The Standard Operating Procedures document notes that before officers obtain a probe image, tips are provided 'giving advice on how to obtain the best image possible to allow for OIFR to recognise a face'.[364] However, officers can still use FRT and search an unsuitable low-quality probe image against the watchlist. In fact, the equality impact assessment (EIA) notes that on several occasions OIFR was used more than once with the same subject, for instance, because one subject 'was wearing clothing that obstructed his face' and another subject 'was photographed in a very dark street at night with very little lighting'.[365] These examples indicate that an unsuitable probe image was obtained and used with OIFR.	
D. Have police pre-established and met thresholds for the FRT system's accuracy (precision, false positive rate, true positive rate) to inform the legal test of strict necessity for personal data processing?	0 / 1
Notes: SWP has not pre-established thresholds for OIFR's accuracy in their published documents. Even though OIFR is shown to perform well in SWP's evaluations, it is still critical to pre-establish thresholds for accuracy to inform the legal test of necessity.	
	0 / 2

Deployment Performance (Equality Act 2010)	Score
E. Does FRT perform well (precision, false positive rate, true positive rate) and similarly across demographic groups?	1 / 1
Notes: SWP's EIA states that 'On every occasion the image searched within app returned a match for the subject, regardless of Ethnicity, Gender, or age and ranked the subject as the number one result without exception'.[366] This indicates that OIFR performed well and similarly across demographic groups.	
	1 / 1

[363] South Wales Police and Gwent Police, 'Operator Initiated Facial Recognition (OIFR) Legal Mandate', p. 9.

[364] South Wales Police and Gwent Police, 'Standard Operating Procedures for the Overt Use of Operator Initiated Facial Recognition (OIFR)', p. 8.

[365] South Wales Police, 'Equality Impact Assessment: Facial Recognition Technology – Retrospective, Live and Operator Initiated', p. 21.

[366] South Wales Police, 'Equality Impact Assessment: Facial Recognition Technology – Retrospective, Live and Operator Initiated', p. 21.

F.3 Human decision-making

Human Review	Score
A. Is there a transparent evaluation that shows human review of the FRT matches is reliable, given the accuracy of officer-verified matches and the amount of time an officer has to review an FRT match?	0 / 1
Notes: There is no published evaluation that shows human review of the OIFR matches is reliable. Even though the equality impact assessment indicates that OIFR performs very well, there is no assessment of how reliably police officers review the OIFR matches, and it is not clear how much time officers have to review OIFR matches.[367] The lack of an evaluation of the human decision-maker raises concerns about whether there is a reliable 'human in the loop' for the use of OIFR in policing.	
	0 / 1

Preparation	Score
B. Is training for the particular type of FRT mandated for police officers using the technology?	1 / 1
Notes: The Standard Operating Procedure notes that, 'All SWP/GWP officers and staff involved in the use of OIFR must receive OIFR training prior to use.[368]	
C. Are there clear standards for technical training on using FRT, data protection training, and training on risks including differential treatment, function creep, and unwarranted intrusions?	0 / 1
Notes: The standards for OIFR training are not very clear. The Policy Document notes that, 'Operators are trained to understand the risks associated with use of the software, including how potential injustices may be caused through inappropriate responses, and that they are accountable for their actions'.[369] The DPIA also notes that, 'As part of OIFR training appropriate data protection training will be provided.'[370] However, no further details about the training standards are provided. For example, it is not clear what specific risks and potential injustices associated with OIFR are included in the training.	
D. Has there been a documented non-operational research trial of FRT with informed consent from participants before the operational use of FRT for policing?	1 / 1
Notes: SWP's equality impact assessment (EIA) documents a non-operational research trial of OIFR. The purpose of this trial was to internally test the performance of OIFR. This trial was conducted with SWP staff and warranted officers who provided 'written consent for their images to be used to create a watch list and for a photograph of themselves to be taken in person via the application for comparison against the said watch list'.[371] This trial was conducted in November 2021 before the operational use of OIFR for policing purposes. The trial results are also reported in the EIA: 'On every occasion the image searched within app returned a match for the subject, regardless of Ethnicity, Gender, or age and ranked the subject as the number one result without exception'.[372] While these results indicate good technical performance, we note that the demographic makeup of trial subjects is unknown.	
	2 / 3

[367] South Wales Police, 'Equality Impact Assessment: Facial Recognition Technology – Retrospective, Live and Operator Initiated'.

[368] South Wales Police and Gwent Police, 'Standard Operating Procedures for the Overt Use of Operator Initiated Facial Recognition (OIFR)', p. 15.

[369] South Wales Police and Gwent Police, 'Policy Document for the Overt Use of Operator Initiated Facial Recognition (OIFR)', p. 13.

[370] South Wales Police and Gwent Police, 'Operator Initiated Facial Recognition (OIFR) Legal Mandate', p. 38.

[371] South Wales Police, 'Equality Impact Assessment: Facial Recognition Technology – Retrospective, Live and Operator Initiated', p. 21.

[372] South Wales Police, 'Equality Impact Assessment: Facial Recognition Technology – Retrospective, Live and Operator Initiated', p. 21.

Accountability	Score
E. Are there clear measures for police to document cases of harm resulting from the use of FRT such as differential treatment, function creep, or unwarranted intrusions?	0 / 1
Notes: There are no clear measures to report cases of harm. SWP's deployment results do not include any evaluations of differential treatment, function creep, or unwarranted intrusions. For example, OIFR was used on 35 persons, and there were 20 reported outcomes (11 arrests, 4 summons for offences, 5 safeguarding measures).[373] The outcomes for the remaining 15 people were not provided, and it is not clear if they faced any unwarranted intrusions such as being stopped and searched.	
F. Do police have a whistleblower protection policy to protect persons who reveal FRT misuse?	1 / 1
Notes: SWP has a whistleblower protection policy that articulates the procedures regarding confidentiality.[374]	
G. Is there a clear redress mechanism (beyond judicial review and usual complaint procedures) for harmed individuals and groups to participate in an investigation into police use of FRT?	0 / 1
Notes: There is no clear redress mechanism for those harmed. The OIFR documents do not indicate clear lines of accountability: (1) The Policy document notes that, 'Operators are trained to understand […] how potential injustices may be caused through inappropriate responses, and that they are accountable for their actions.' [375] However, it is not clear how officers are held accountable. (2) The Policy document also states that, 'The Divisional Services Division Chief Superintendent […] is responsible for effective governance and accountability for the OIFR pilot'.[376] However, it is not clear what this accountability entails and what measures are taken in the case of harm. (3) The appropriate policy documents include technical and organisational measures for the accountability principle of the Data Protection Act 2018. However, there are no measures mentioned with regard to a process for accountability in the case of harm. This lack of clarity on redress and accountability is confirmed by the House of Lords Justice and Home Affairs Committee report on new technologies in the justice system that highlights the lack of recourse for people harmed by the use of technologies such as FRT.[377]	
H. Are there clear measures to ensure that the redress mechanism is procedurally fair?	0 / 1
Notes: There are no clear measures to ensure a procedurally fair redress mechanism; there is no clear redress mechanism in the first place.	
	1 / 4

[373] South Wales Police, 'Facial Recognition App Pilot Results'.

[374] South Wales Police, 'Whistleblowing: Guidance & Procedure Summary'.

[375] South Wales Police and Gwent Police, 'Policy Document for the Overt Use of Operator Initiated Facial Recognition (OIFR)', p. 13.

[376] South Wales Police and Gwent Police, 'Policy Document for the Overt Use of Operator Initiated Facial Recognition (OIFR)', p. 13.

[377] House of Lords, Justice and Home Affairs Committee, *Technology Rules?*, p. 37.

F.4 Expertise and oversight

Ethics Committee	Score
A. Is regular oversight from an ethics committee mandated throughout the life of the FRT project?	1 / 1
Notes: SWP's equality impact assessment highlights oversight provided from the SWP Joint Independent Ethics Committee before and after the OIFR trial: 'Briefings took place with the committee in November 2021 and March 2022. The pilot of the OIFR app was predominantly presented to the group, but all areas of Facial Recognition Technology was discussed. The grounds and reasons for use of the app were relayed including use cases and when the app can be expected to be used […] During the follow up meeting in March 2022 following the end of the 3 month pilot, the results and use cases along with lessons learnt were also discussed. The group posed questions to the project team around use of the app, scrutiny of the app, lessons learnt and progression. Positive feedback and support was received with a commitment made by the project team to further engage with the group at the next relevant time and stage'.[378]	
B. Are there clear processes for the committee to influence if and how FRT is implemented, including the power of veto for the FRT project?	0 / 1
Notes: The SWP Joint Independent Ethics Committee is advisory, and there are no clear processes for the committee to influence if and how FRT is implemented, including the power of veto. With regard to the committee's feedback, SWP's equality impact assessment states that, 'The grounds and reasons for use of the app were relayed including use cases and when the app can be expected to be used. In addition, the scrutiny placed on uses and each use including the use of body worn video and subsequent reviews, officer engagement and feedback was also relayed'.[379] However, the specific feedback from the committee on the implementation of OIFR is not published, and it is not clear whether and how this feedback influenced the implementation of OIFR. The committee's Terms of Business are not published, but the SWP website states that the committee provides advice, support and assistance.[380] Thus, the nature of the committee is advisory and likely lacks decision-making power, including the power of veto.	
C. Is the committee an independent body from police organisations with members having non-policing backgrounds and with safeguards to ensure the committee's sustainability even without political support?	0 / 1
Notes: The SWP Joint Independent Ethics Committee is not an independent body, as it is situated within South Wales Police. Although the committee includes some independent members, the committee also includes police officers (Chief Officer and Chief Superintendent).[381] We also examined the members listed in the most recently published meeting minutes (June 2021); of the 20 individuals in attendance or apologies (invited but unable to attend), 11 (55%) were members of SWP and 12 (60%) were either a member of SWP or the South Wales Police and Crime Commissioner.[382] Finally, the committee's Terms of Business are not published, and it is not clear what safeguards are in place to ensure the committee's sustainability.	

[378] South Wales Police, 'Equality Impact Assessment: Facial Recognition Technology – Retrospective, Live and Operator Initiated', p. 23.

[379] South Wales Police, 'Equality Impact Assessment: Facial Recognition Technology – Retrospective, Live and Operator Initiated', p. 23.

[380] South Wales Police, 'Our Vision, Values, and Ethics'.

[381] South Wales Police, 'Our Vision, Values, and Ethics'.

[382] South Wales Police Joint Independent Ethics Committee, 'Meeting Minutes, 10 June 2021' <https://www.south-wales.police.uk/SysSiteAssets/media/images/south-wales/about-us/stats-and-data/joint-independent-ethics-committee-minutes---june-2021.pdf> [accessed 17 July 2022].

Ethics Committee (continued)	Score
D. Is the committee diverse in terms of demographic makeup and independent expertise in human rights, equality, and data protection?	0 / 1
Notes: The demographic diversity of the SWP Joint Independent Ethics Committee is not published. We also researched the backgrounds of the committee members listed in the most recently published meeting minutes (June 2021) and found that there were no independent experts in human rights, equality, or data protection.[383] Based on recruitment materials for the appointment of members to the committee, there is no indication that demographic diversity is considered in the selection of members nor that expertise in human rights, equality, or data protection is considered.[384]	
E. Are detailed meeting minutes published, including briefing papers, discussions, and conclusions?	0 / 1
Notes: The South Wales Joint Independent Ethics Committee's minutes for the November 2021 to March 2022 meetings where OIFR was discussed have not been published as of the audit evaluation date (July 2022). While SWP's EIA mentions some points that were discussed with the South Wales Joint Independent Ethics Committee, briefing papers and the details of discussions and conclusions are not publicly available, despite the OIFR trial having already been completed.	
	1 / 5

Civil Society and Experts	Score
F. Are there transparent, proactive consultations with civil society and independent experts on the particular type of FRT?	0 / 1
Notes: There are a few issues of concern based on the consultations documented in the DPIA. (1) There are no consultations with civil society on the use of OIFR. (2) It is unclear when and how frequently consultations occurred. This is critical to assess whether they were proactive. (3) There is a lack of transparency about consultations. For example, SWP consulted the Surveillance Camera Commissioner and Biometrics Camera Commissioner. The DPIA indicates that there was 'professional discussion over project proposals and implementation' with both commissioners, but the feedback provided and the outcome of these consultations are not transparent.[385] (4) Several of the consultations are indirect and in reference to LFR rather than OIFR. For example, out of a total of 15 consultations, consultations with the following four stakeholders focus on LFR: Information Commissioner's Office, College of Policing, Ada Lovelace Institute, and London Policing Ethics Panel.[386]	
G. Are police required to consider the advice from consultations and transparently explain the outcomes, including providing a justification if the advice is not followed?	0 / 1
Notes: There is no documentation that SWP is required to consider the advice from consultations. Based on the consultations documented in the DPIA, SWP does not indicate and justify if guidance from a consultation was not followed. There is little documentation of the outcome and influence of consultations.	
	0 / 2

[383] South Wales Police Joint Independent Ethics Committee, 'Meeting Minutes, 10 June 2021'.

[384] South Wales Police Corporate Services, *Briefing Pack*; South Wales Police and Crime Commissioner and Chief Constable, 'Appointment of Members to *The Independent* Ethics Committee'; South Wales Police and Crime Commissioner and Chief Constable, 'Person Specification – Independent Ethics Committee'.

[385] South Wales Police and Gwent Police, 'Data Protection Impact Assessment for Operator Initiated Facial Recognition (OIFR)', p. 16.

[386] South Wales Police and Gwent Police, 'Data Protection Impact Assessment for Operator Initiated Facial Recognition (OIFR)', pp. 16–17.

Community Engagement	Score
H. Are there clear, proactive processes for the public, especially marginalised communities, to influence if and how FRT is implemented?	0 / 1
Notes: There were no clear, proactive processes for the public to influence if and how OIFR was implemented. Based on the consultations documented in the DPIA, there were no direct consultations with the public, especially marginalised communities, on the use of OIFR before or during its deployment.	
I. Are all FRT materials accessible to people with disabilities and provided in immigrant languages?	0 / 1
Notes: The OIFR documents on the SWP website may not be accessible to people with disabilities. As of the audit evaluation date (July 2022), the SWP website is not fully compliant with accessibility regulations: 'This website is partially compliant with the Web Content Accessibility Guidelines version 2.1 AA standard, due to the non-compliances listed below [...] PDFs may not be suitable for users of assistive technology. We are in the process of replacing or fixing any PDF and Word documents which are essential to our services, however users can request accessible versions'.[387] The OIFR documents are also not provided in immigrant languages. Some information is provided in Welsh but not in any immigrant languages. These accessibility issues can pose barriers to certain communities and make it difficult to understand the use and impact of OIFR.	
	0 / 2

[387] South Wales Police, 'Accessibility' <https://www.south-wales.police.uk/hyg/accessibility/> [accessed 16 July 2022].

MINDEROO CENTRE FOR TECHNOLOGY & DEMOCRACY

Alison Richard Building
7 West Road, Cambridge
CB3 9DT

www.mctd.ac.uk

minderoo@crassh.cam.ac.uk

UNIVERSITY OF CAMBRIDGE

Report design by **CHRIS PRINTED THIS**

Images taken from Unsplash and Pexels courtesy of Cottonbro, Alex Knight, Charles Deluvio, Gayatri Malhotra, Kalea Morgan, James Eades, Levi Meir Clancy, King's Church International, Kyle Bushnell, Tobias Tullius, Paul Silvan, The Blowup, Ehimetalor Akhere, Jonny Gios, Claire Dornic, Anna Dziubinska, Robert Tudor, Kyle Hinkson, Robin Worrall, Jake Weirick, Nathy Dog, The New York Public Library, and Arthur Edelmans.