Prof. Pete Fussey, Dr. Daragh Murray, Dr. Amy Stevens, University of Essex[1]— Written evidence (NTL0017)

1. We welcome the opportunity to contribute to the Committee's work. This submission primarily responds to questions 2, 3, 5 and 7. However, it is hoped that the issues raised will also inform the development of any principles, as highlighted in question 10.

2. The issues addressed are as follows:

a. The requirement that police deployment of new and emerging technologies be 'in accordance with the law', and regulated by means of dedicated legislation;
b. Operational issues relating to *how* the use of new and emerging technologies influences policing practices;
c. Bias and transparency;
d. The need for a comprehensive human rights impact assessment, distinct from and wider ranging than a data protection impact assessment;
e. The need to demonstrate the utility of any new and emerging technologies, drawing on an appropriate evidence base;
f. The need to meaningfully review human decision-making.

3. This submission primarily draws on the authors' experience of empirically researching police use of facial recognition technology. However, a number of the points raised are relevant to police uses of other new and emerging technologies, which have also been analysed through academic empirical fieldwork.

The use of new technology must have a legal basis

4. It is broadly accepted that police adoptions of new technologies that utilise artificial intelligence or algorithmic decision making bring into play (or 'engage') a number of human rights.[2] To-date, attention has focused primarily on the right to privacy,[3] and the prohibition of discrimination.[4] However, depending on the manner in which these technologies are deployed, other rights may also be engaged, such as: the right to freedom of expression;[5] the right to freedom of assembly and association;[6] and the right to freedom of thought, conscience and religion.[7]

5. In order to be lawful, any interference with these rights must satisfy a three-part test. The interference must be:

[1] Research underpinning this submission has been funded by UKRI ESRC Project Human Rights, Big Data and Technology ES/M010236/1 (Fussey and Stevens); and a UKRI Future Leaders Fellowship MR/T042133/1 (Murray)
[2] See further, Human Rights, Big Data & Technology Project, 'Putting Human Rights at the Heart of the Design, Development and Deployment of Artificial Intelligence', 20 December 2018.
[3] Article 8, European Convention on Human Rights.
[4] Article 14, European Convention on Human Rights; Chapter 2, Equality Act 2010.
[5] Article 10, European Convention on Human Rights.
[6] Article 11, European Convention on Human Rights.
[7] Article 9, European Convention on Human Rights.

- In accordance with the law;
- In pursuit of a legitimate aim;
- Necessary in a democratic society.[8]

6. Police use of new and emerging technologies must satisfy this three-part test. It is our opinion that – with respect to the deployment of many new technologies that impact human rights protections – the 'in accordance with the law' test cannot be satisfied in the absence of dedicated legislation[9] (similar, for example, to the regulation of modern surveillance practices by means of the Investigatory Powers Act 2016).

7. For facial recognition surveillance, this conclusion is reinforced by the Court of Appeal judgment in *Bridges*. Here, the Court rejected the claim that an adequate legal framework existed for South Wales' Police use of live facial recognition (LFR) technology.[10] The Court of Appeal noted that:

> The fundamental deficiencies, as we see it, in the legal framework currently in place relate to two areas of concern. The first is what was called the "who question" at the hearing before us. The second is the "where question". In relation to both of those questions too much discretion is currently left to individual police officers. It is not clear who can be placed on the watchlist nor is it clear that there are any criteria for determining where AFR [automatic facial recognition] can be deployed.[11]

8. Similar questions are likely to be raised with respect to police use of other new and emerging technologies. It is our opinion that the answers to questions such as these should be established in legislation. In particular, and in order to avoid arbitrary rights interferences, national legislation should clearly set out: the circumstances in which a new technology may be used[12] (ensuring that use is limited to that which is 'necessary in a democratic society'[13]), the framework for authorising a deployment, and the supervisory and accountability mechanisms.

9. It is important to consider how technology may be deployed in a number of different ways and contexts. A change in the nature of a deployment may result in significantly different benefits to law enforcement and/or significantly different harm to human rights. For example, facial recognition technology may be deployed at a border crossing, in order to verify an individual's identity. Equally, facial recognition technology may be deployed across a city-wide surveillance camera network and used to track individuals' movements throughout time.[14]

---

[8] See, e.g. *Big Brother Watch and Others v. the United Kingdom*, Grand Chamber, ECtHR, App. Nos. 58170/13, 62322/14 & 24960/15, 25 May 2021, para. 332.
[9] See, for example, Prof. Pete Fussey & Dr. Daragh Murray, 'Independent Report on the London Metropolitan Police Service's Trial of Live Facial Recognition Technology', Human Rights, Big Data & Technology Project, June 2019, section 3.2.
[10] *Bridges v. South Wales Police* [2020] EWCA Civ 1058, Case No. C1/2019/2670, 11 August 2020, para. 90.
[11] *Bridges v. South Wales Police* [2020] EWCA Civ 1058, Case No. C1/2019/2670, 11 August 2020, para. 91.
[12] This is a means of addressing questions such as those raised in *Bridges,* relating to the 'who', 'what', 'where' and 'when' of any deployment of new technology.
[13] See, e.g., *Centrum For Rattvisa v. Sweden*, Grand Chamber, ECtHR, App. No. 35252/08, 25 May 2021, para. 248; *Big Brother Watch and Others v. the United Kingdom*, Grand Chamber, ECtHR, App. Nos. 58170/13, 62322/14 & 24960/15, 25 May 2021, para. 334.

Although both deployments involve the use of facial recognition technology the impact on individuals' human rights is markedly different. Evidently, the circumstances in which technologies are deployed will have a significant impact on the 'necessary in a democratic society' calculation. There is no generic single application of this technology and it is important that underlying legislation clearly circumscribes the permissible parameters of use.

10. It is the authors' opinion that public policies or codes of practice cannot be substituted for legislation. With respect to new technologies exerting a significant impact on human rights protections legislation is required in order to ensure conformity with the 'in accordance with the law' requirement established in the Human Rights Act. This legislation can then be supplemented by public policy or codes of practice.

11. It is also the case that many technologies are adopted without guiding codes of practice setting out consistent and appropriate use. At one level this illustrates a wider problem of insufficient governance and oversight of potentially intrusive technologies.

12. In addition, our research examining how police use advanced technologies[15] in operational settings found that the absence of clear guidance and oversight created significant dilemmas for those officers. In particular, officers became responsible for continuously evaluating the applicability of any analogous guidance, which added to the strain of using such tools and engendered highly inconsistent practices.[16] In this sense, oversight and guidance would therefore provide a means to facilitate more effective policework.

Operational Issues

13. Issues arising regarding the operational use of technology for law enforcement remain largely unaddressed. These draw attention beyond the 'who' and 'where' questions outlined above to also address 'how' technology is actually being used operationally. Fully understanding how a technology is used in practice may introduce additional concerns.

14. There is a need to ensure that new technologies are not simply seen as 'upgrades' to existing practices or tools. While certain new technologies may be a continuation of existing practices or tools by other means, other technologies will mark a step change in police capabilities or will introduce new human rights considerations. These considerations are important for the application of the 'necessary in a democratic society' test.

15. For example, LFR can be deployed across a public surveillance camera network, allowing for the identification and tracking of every individual who passes through the camera network's field of vision. This ability to identify and

[14] The potential also exists for this information to be fused with other sources of data, and subject to advanced analytics.
[15] Technologies included predictive policing, social media analysis, online covert operations and advanced biometric surveillance.
[16] Fussey, P., and Sandhu, A. (2021 in press) 'Surveillance Arbitration in the era of Digital Policing', *Theoretical Criminology*, available open access: https://journals.sagepub.com/doi/10.1177/1362480620967020

track large numbers of individuals on a 24/7 basis is simply impossible using traditional police resources, and so the use of LFR in this context arguably constitutes a step change in police capability. Conversely, the use of facial recognition technology to verify the identity of an individual at a border crossing arguably represents a continuation of traditional policing practices.

16. Operational factors will also influence 'how' policing is conducted, with potentially significant implications both with respect to human rights impacts, and policing effectiveness. This may be illustrated with examples drawn from LFR-related research:

- LFR brings subtle yet important shifts in how surveillance is enacted. While most surveillance authorisation and oversight schemes (e.g. RIPA) are designed to target individuals once a threshold of suspicion has been reached, LFR operates in a different manner. With facial recognition, everybody who passes through space is considered equally suspicious in the first instance and is then eliminated from enquiries, much like mass DNA sampling in the search for suspects. In this sense, LFR should arguably be regarded as a step change in police powers/capabilities, rather than a continuation of existing powers/capabilities and therefore requires levels of authorisation, oversight and accountability that accompany other highly intrusive surveillance measures. The Court of Appeal judgement in *Bridges* was unequivocal in its criticism of excessive police discretion surrounding South Wales Police's use of LFR. It would follow that decisions over the use of this technology should be auditable and held to external scrutiny.
- Published academic research based on the only independent analysis of operational uses of LFR, and researched over multiple sites, establishes that this technology affects how officers see suspicion.[17] In particular, the evidence establishes that computer-originated LFR matches frame the way those matched are seen as suspicious, a process described elsewhere as a 'presumption to intervene'.[18] This works in a way psychologists may describe as 'priming', where individuals become more likely to act in specific ways due to prior exposure to particular stimuli. As such, any LFR uses would need to have an ongoing audit of decision making, and training processes, to understand these effects and to mitigate the risk of arbitrary and flawed interventions with innocent passers-by. This suggests that attention should also be paid to whether the same presumptive processes apply elsewhere. This is of particular importance when the use of new technologies, such as algorithmic decision-support tools are intended only to be 'advisory' in nature. An example of such use is Durham Constabulary's Harm Risk Assessment Tool (HART) which aids decisions made by custody officers by providing forecasts for the likelihood of reoffending.[19] In such situations, any

[17] Fussey, P., Davies, B. and Innes, M., (2021). 'Assisted' Facial Recognition and the Reinvention of Suspicion and Discretion in Digital Policing. The British Journal of Criminology. 61 (2), 325-344

[18] Fussey, P., and Murray, D. (2020) 'Policing Uses of Facial Recognition in the UK', in A. Kak (ed.) *Regulating Biometrics: Global Approaches and Urgent Questions*, AI NOW: AI NOW/New York University

[19] For more information see: Oswald, M, Grace, J, Urwin, S and Barnes G (2018) 'Algorithmic risk

potential tendency to defer or over-rely on automated outputs over other available information has the ability to transform what is still considered to be a human-led decision to de facto an automated one. Robust monitoring should therefore be in place to provide an understanding of the level of deference to tools intended as advisory, and how often and in which circumstances human users make an alternative decision to the one advised by the tool.

Bias and Transparency

17. Bias in facial recognition algorithms and differential performance across different ethnic, gender and age categories are established scientific facts. Such bias/disparity was established in the most wide-ranging evaluative study ever conducted on this issue,[20] carried out by the US Federal Government National Institute of Standards and Technology (NIST). NIST found these disparities in 189 different algorithms. Indeed, scientific evaluator's repeatedly caution users to "know your algorithm" in recognition of these disparities.

18. Knowledge of such deficiencies is therefore crucial for users to fulfil their positive obligation under the Public Sector Equality Duty (PSED). The finding of the Court of Appeal in *Bridges* is highly relevant: "Dr Jain cannot comment on this particular software but that is because, for reasons of commercial confidentiality, the manufacturer is not prepared to divulge the details so that it could be tested. *That may be understandable but, in our view, it does not enable a public authority to discharge its own, non-delegable, duty under section 149*"[21] (emphasis added). This suggests that if the police cannot verify that the software can be deployed in line with the PSED, the software should not be deployed. It is also important to emphasise that the *Bridges* Court of Appeal held that: 'all police forces that intend to use it [LFR] in the future would wish to satisfy themselves that everything reasonable which could be done had been done in order to make sure that the software used does not have a racial or gender bias',[22] and that a public authority should 'acquire relevant information in order to conform to the PSED and, in particular, to avoid indirect discrimination on racial or gender grounds.'[23] This reasoning is equally applicable to other law enforcement uses of new and emerging technology.

19. Ongoing measures of auditability should also be considered. With respect to LFR, for example, this could include the logging of LFR-induced ID checks on people akin to post-MacPherson changes to capturing ethnicity during stop and search.

Human rights assessment

---

assessment policing models: lessons from the Durham HART model and 'Experimental' proportionality' *Information and Communications Technology Law* (27)2.

[20] The report is available here: https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf

[21] *Bridges v. South Wales Police* [2020] EWCA Civ 1058, Case No. C1/2019/2670, 11 August 2020, para. 199. Emphasis added.

[22] *Bridges v. South Wales Police* [2020] EWCA Civ 1058, Case No. C1/2019/2670, 11 August 2020, para 201.

[23] *Bridges v. South Wales Police* [2020] EWCA Civ 1058, Case No. C1/2019/2670, 11 August 2020, para 2010.

20. A full assessment of potential harm is essential. It is well established in the scholarship on this issue that, while useful, data protection (and, by extension, Data Protection Impact Assessments) is an incomplete way of capturing the range of potential harms. Depending upon the deployment, potential human rights harms extend beyond privacy to include other human rights protections that may foreseeably be engaged by facial recognition deployments, such as the rights to freedom of expression, freedom of assembly and association, and freedom of religion.[24]

Utility

21. The utility of technology in relation to the solving of crime and other social issues is frequently assumed or overestimated in the absence of evidence which proves its ability to do the task that it has been developed or marketed to do, or indeed in the conditions in which it would be used in practice.

22. For example, the utility of LFR is often assumed, i.e. through claims that it will be able to address whatever crime problem/legitimate aim is presented, by virtue of its inherent (unproven) ability. Without questioning its limitations (use in poor light or in specific spaces) this tilts the calculus towards it always being considered necessary. Yet research of its operational uses exists to challenge this assumption. As such, we contend that the operational case for LFR has not been made.

23. We would also suggest a requirement for considering prior experiences/learning as new technology is deployed and developed. For example, during our LFR research we encountered instances where, despite indications that the system was not working well (on any measure), it was repeatedly deployed for the same purpose.[25]

24. As such, the case to support the use of facial recognition – or any other new technology – should be established prior to deployment. This justification should be evidenced with recourse to scientific fact, recorded and be capable of being considered and evaluated by an objective third party. Justifications should also be tailored to the specific purposes for which the technology is deployed and with reference to the specific circumstances and contexts in which it is intended to be used. Moreover, if such justifications cannot be provided then the case for using such technologies has not been made.

25. It is worth emphasizing, for example, that there is therefore no 'one size fits all' approach to LFR. This is because the potential human rights harm will vary significantly dependent upon the nature of each deployment. Any change to the

---

[24] See, for instance, Fussey, P. and Murray, D., (2019). Independent Report on the London Metropolitan Police Service's Trial of Live Facial Recognition Technology, University of Essex Human Rights Centre, available here: http://repository.essex.ac.uk/24946/1/London-Met-Police-Trial-of-Facial-Recognition-Tech-Report-2.pdf; Purshouse, J. and Campbell, L. (2019) 'Privacy, Crime Control and Police Use of Automated Facial Recognition Technology', *Criminal Law Review*, vol. 3: 188-204

[25] Fussey, P. and Murray, D., (2019). Independent Report on the London Metropolitan Police Service's Trial of Live Facial Recognition Technology, University of Essex Human Rights Centre, available here: http://repository.essex.ac.uk/24946/1/London-Met-Police-Trial-of-Facial-Recognition-Tech-Report-2.pdf

focus and form of a deployment may give rise to a potentially significant change in the human rights impact. This may affect the level of interference with a particular right, and/or the number of rights brought into play (including freedom of association, etc.).

26. Appropriate police policy documents – setting out the claimed utility associated with the deployment of a new technology and the potential harm of that deployment – are also a means of facilitating compliance with the 'necessary in a democratic society' test. Simply put, if the potential utility of a new police technology is not set out, and the circumstances of the deployment are not delimited, then it is impossible to effectively engage with the 'necessary in a democratic society' test.

27. The audit trail is important for accountability purposes, but it is also a means of proactively working to ensure compliance with human rights law, and more directly incorporating human rights considerations into the formulation of police policy.

The Need to Review Human Decision Making

28. We suggest that good practice would include some post hoc and auditable review of 'human-in-the-loop' adjudication outcomes to inform future practices.

29. It is important to highlight the need for a consistent approach towards technology supported decision-making. With regards to facial recognition technology, we found significant variation in human adjudication arrangements in our research. Sometimes two people made a decision, sometimes one, sometimes a group. Sometimes decisions were made in front of the laptop screen, sometimes on the street. The result of this was often that whenever a choice was made to apprehend someone on the street any voice which confirmed the algorithm was upheld. Conversely, decisions not to intervene and stop an individual were often overturned. A more consistent approach will allow more consistent treatment of these deliberations and ensure that there is not a tendency to defer to automated outputs when alternative available information suggests a different course of action may be more appropriate. This also ensures transparency, that tools that are intended to aid human decision makers – and are publicly presented as such – do just that and do not instead become the de facto decision makers.

30. While the existence of human decision-making is a legal requirement under the Data Protection Act 2018, it is not necessarily the existence of human adjudication that is at question, but the nature, quality and degree of such judgements.

31. It is important that understanding vis-à-vis both the underlying technology, and the role of the human operator, be included in any training.

3 September 2021