UNIVERSITY OF CAMBRIDGE

Bennett Institute for Public Policy
Cambridge

BENNETT INSTITUTE WORKING PAPER

Governing Live Automated Facial Recognition Systems for Policing in England and Wales

December 2020

By
Fengyu (Isabella) Duan

ABSTRACT

The use of live automated facial recognition (AFR) systems in England and Wales for law enforcement purposes has been the subject of criticism concerning the inadequacy of governance of the technology. Defining the ideal governance framework as one that sustains well-placed societal trust, improved governance must ensure that the use of the AFR systems in policing is validated by evidence justifying its efficacy, and by the demonstration of the evidence to the public as well as expert stakeholders. Drawing on interviews with stakeholders from government, industry, civil society and the police, this essay contributes to public policy literature on technology governance, exploring governance through the lens of trust.

INTRODUCTION

Since 2016, English and Welsh police forces pioneered by the South Wales Police (SWP) and the Metropolitan Police Service (MPS) have been conducting trials for live automated facial recognition (AFR) technology.[1] In August 2020, the Court of Appeal reviewed the case *Bridges v. the Chief Constable of the SWP and Others* and ruled that the SWP's deployment of AFR did not have an adequate legal framework. Welcoming the legal challenge as a rigorous test of their policy, both the SWP and the MPS announced they plan to continue the deployment and development of AFR systems in light of the Court's judgement.

While the law defines the 'lawful', it may not define the 'ideal', or the best state of affairs for society. This essay defines the 'ideal' for AFR systems as 'well-trusted', which means they are both trustworthy and trusted. In 2018, the Home Office outlined the ambition of delivering better service while maintaining public trust as its biometrics strategy.[2]

[1] Following the devolution of policing power, the use of live AFR systems in the Northern Ireland and Scotland is not under the control of the UK parliament and government at Westminster. Police Service of Northern Ireland has not used any facial recognition system, whereas the Scottish Parliament has held that "there would be no justifiable basis for Police Scotland to invest live AFR systems.

See Police Service of Northern Ireland, "Freedom of Information Request: F-2020-00188". Accessed November 1, 2020, https://www.psni.police.uk/globalassets/advice--information/our-publications/disclosure-logs/2020/organisational-informal-and-governance/00188-facial-recognition-technology.pdf.

See also The Scottish Parliament, "Facial Recognition: How Policing in Scotland Makes Use of This Technology." Accessed November 1, 2020, https://digitalpublications.parliament.scot/Committees/Report/JSP/2020/2/11/Facial-recognition--how-policing-in-Scotland-makes-use-of-this-technology.

[2] The UK's Home Office, "Biometrics Strategy: Better public services and Maintaining public trust," (June 2018), 13. Accessed September 19, 2020,

Placing trust well, that is, to trust the trustworthy and to distrust the untrustworthy, is the ideal for democratic citizens. Trust forms an important lens through which the public view AFR systems.[3] People's assessment of the trustworthiness of the police is also a reliable indicator of police legitimacy and public cooperation with policing.[4] Therefore, well-placed trust is a powerful analytical concept describing an ideal relationship between the public and the government or its agent such as the police.

The literature on trust comprises a variety of disciplines including philosophy, sociology, organisational sciences, economics, and psychology. I understand *trust* as an epistemic attempt of the trustor, an active inquiry not passive acceptance, and distinguish trust from *trustworthiness*, which concerns the nature of the trustee.[5] Trust does not have to be symmetrical, as opposed to a mutually trusting relationship. Nor does trust have to be validated. Indeed, the component of risk-taking is fundamental, for trust would be redundant if there is no risk of disappointment. To trust is to think and act as if one could not be disappointed.[6] Trust is *well-placed* when that as-if assumption is valid, that is,

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/720850/Home_Office_Biometrics_Strategy_-_2018-06-28.pdf.

[3] London Policing Ethics Panel, "Final Report on Live Facial Recognition," (May 2019), 7. Accessed September 19, 2020, http://www.policingethicspanel.london/uploads/4/4/0/7/44076193/live_facial_recognition_final_report_may_2019.pdf.

[4] Jackson, Jonathan and Hough, Mike and Bradford, Ben and Hohl, Katrin and Kuha, Jouni, "Policing by consent: understanding the dynamics of police power and legitimacy," *ESS country specific topline results series 1*, (2012). European Commission. Accessed September 19, 2020, http://eprints.lse.ac.uk/47220/1/Policing%20by%20consent(lsero).pdf.

[5] Onora O'Neill, A Question of Trust: The BBC Reith Lectures 2002 (Cambridge: Cambridge University Press, 2002).

[6] Philip Pettit, "The cunning of trust," Philosophy & Public Affairs 24, no. 3 (1995): 202-225.

when there is subsequent evidence about the trustworthiness of the trustee,[7] in this case, the AFR socio-technical systems that incorporate not only the algorithms but also the human operators and the broader governance and accountability framework.

Drawing from interviews with 23 stakeholders from the government, industry, academia, civil society, and the police as well as archive data, I analyze and contrast ways in which different stakeholders and the public decide to place trust (or not) in police's use of AFR systems. Identifying substantial differences among stakeholders that have frustrated the evaluation of trustworthiness and might have eroded public trust,[8] I argue that to ensure well-placed societal trust, a good governance framework must coordinate the accumulation, evaluation, and demonstration of evidence among stakeholders. Towards that end, I summarize recommendations for policy reform.

[7] Onora O'Neill, 'Linking Trust to Trustworthiness,' *International Journal of Philosophical Studies 26*, no. 2 (2018).

[8] Open Data Institute, "Designing trustworthy data institutions," (2020). Accessed September 26, 2020, http://theodi.org/wp-content/uploads/2020/04/OPEN_Designing-trustworthy-data-institutions_ODI_2020.pdf.

CONTEXT

This section discusses contexts in which stakeholders and the public in England and Wales place trust in the police. There are different ways of placing trust and different interpretations of trustworthiness, depending on a community's accepted way of knowing and constitutive of the community's collective identity. Despite an emerging global convergence on some principles for artificial intelligence and other data-driven technologies, such as transparency, justice and fairness, non-maleficence, responsibility and privacy, there are significant semantic and conceptual divergences in how these principles are interpreted by different public sector organizations, private companies, research institutions, and the public in different national contexts.[9]

The cultural history of policing and data protection governance in England and Wales importantly, although by no means exhaustively, defines but at the same time confuses whether the police's use of AFR systems is trustworthy such that trust placed in the system is valid. The long-standing model of British policing is "policing by consent", meaning that the power of the police is derived from the respect and approval of the public more than from the force of the state.[10] Unlike consent in commercial settings, consent to the law enforcement authority must exist collectively, not individually. The

[9] A. Jobin, M. Ienca, and E. Vayena, "The global landscape of AI ethics guidelines," *Nat Mach Intell 1* (2019): 389–399.

[10] Home Office, "FOL release: Definition of policing by consent," (December 10, 2012). Accessed September 16, 2020, https://www.gov.uk/government/publications/policing-by-consent/definition-of-policing-by-consent.

prevailing assumption is that there is a broad consensus in politics and society on what kind of public order people want the police to maintain.[11] Under this model, public confidence in local police is relatively high, with the majority of survey respondents perceive that the police "do a good or excellent job", act lawfully, and align with their values, despite the majority's perception at the same time that they are not informed about what the police are doing.[12; 13] A similar proportion of people from Black, Asian, and Ethnic Minorities (BAME) backgrounds as White British people have confidence in local police.[14] Therefore, people perceive the police as trustworthy in a general manner, that the police have both the competence and the good intentions to perform the task they are trusted to do, which may entail taking public interests into account in their action, having moral commitments, or having psychological or character disposition to be good police officers.[15]

The trusting relationship between the police and the public suggests that the public might readily have extended trust to new methods of policing. For example, the

[11] Clive Emsley, *The English Police: A Political and Social History* (London: Routledge, 1997), 7.

[12] David Brown and Paul Quinton, "Integrity Programme: Data pack on public trust and confidence in the police," College of Policing, 6-7. Accessed September 16, 2020, https://www.college.police.uk/What-we-do/Ethics/Documents/Data_pack_Public_trust.pdf.

[13] BMG Research, "Public Perception of Policing in England and Wales 2018," (January 2019), 8. Accessed September 16, 2020, https://www.bmgresearch.co.uk/wp-content/uploads/2019/01/1578-HMICFRS-Public-Perceptions-of-Policing-2018_FINAL.pdf.

[14] The UK Government, "Confidence in the local police," (March 4, 2020). Accessed September 16, 2020, https://www.ethnicity-facts-figures.service.gov.uk/crime-justice-and-the-law/policing/confidence-in-the-local-police/latest#by-ethnicity-over-time.

[15] Russell Hardin, Trust (Cambridge: Polity Press, 2006).

exponential growth of state-funded CCTV systems in the UK in the 1990s occurred before any systematic evaluation as to its effectiveness for preventing and detecting crime was carried out.[16] Notwithstanding the subsequent mixed research findings and the distance CCTV operations place between the regulation of public space and the public due to “hidden control rooms”, CCTV systems had gathered widespread public support in the UK and made people feel safe.[17] There was no governance framework restricting the use of CCTV systems, with only limited public engagement on the CCTV policy.[18] Consent was assumed, not sought.

More rigorous regulatory controls, however, have been urged in the context of a growing concern in public debate about the normalization of surveillance. Normative statements which emphasize surveillance feature prominently in the policy discourse, where civil society organizations and other non-state actors are increasingly part of a multi-stakeholder process of policymaking.[19] In this context, consent can no longer be assumed but has to be earned. Nearly half of British people surveyed think that they should be

[16] Clive Norris, “The success of failure. Accounting for the global growth of CCTV,” in Routledge Handbook of Surveillance Studies (2012): 251-258.

[17] Angela Spriggs, Javier Argomaniz, Martin Gill, and Jane Bryan, “Public attitudes towards CCTV: results from the Pre-intervention Public Attitude Survey carried out in areas implementing CCTV,” Home Office Online Report 10/15, (2005), 18. Accessed September 16, 2020, http://library.college.police.uk/docs/hordsolr/rdsolr1005.pdf.

[18] Inga Kroener, “CCTV: A technology under the radar?” PhD Thesis, University College London (2009). Accessed September 22, 2020, https://discovery.ucl.ac.uk/id/eprint/19711/1/19711.pdf.

[19] Arne Hintz, “The politics of surveillance policy: UK regulatory dynamics after Snowden,” Internet Policy Review 5, no. 3 (September 2016): 1-16. DOI: 10.14763/2016.3.424.

able to give or withdraw their consent to the use of AFR systems.[20] For the police's use of the systems specifically, this consent would be contingent upon appropriate safeguards, rather than members of the public assessing the systems themselves.[21] While 96% people in the same survey admit that they know a little or nothing about the police's use of the AFR systems, 67% feel comfortable about such use.[22] This public trust is conditional and conferred by the perceived safeguards.

With significant strides in data protection and privacy legislation in recent decades, there are three elements of safeguards regarding the police's overt deployment of AFR systems.[23] Analogous to policing by consent, "surveillance by consent" first emerged in the Surveillance Camera Code of Practice issued under the Protection of Freedoms Act 2012. Under this legislation, when overt surveillance in public places is used for a specified purpose that is in pursuit of a legitimate aim and meets a pressing need, and when the deployment is proportionate to the stated purpose without unnecessary interference with privacy and other human rights protected under the Human Rights Act 1998, such surveillance is taken to be consented to.[24] In the same year, the Surveillance

[20] Ada Lovelace Institute, "Beyond face value: public attitudes to facial recognition technology," (September 2019), 2. Accessed September 18, 2020, https://www.adalovelaceinstitute.org/wp-content/uploads/2019/09/Public-attitudes-to-facial-recognition-technology_v.FINAL_.pdf.

[21] Ibid.

[22] Ibid.

[23] If used covertly, AFR systems will be regulated in accordance with the provisions of Regulation and Investigatory Power Act 2000 (RIPA) under the guidance of the Investigatory Powers Commissioner.

[24] Home Office, "Surveillance Camera Code of Practice," (June 2013). Accessed September 16, 2020, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/282774/SurveillanceCameraCodePractice.pdf.

Camera Commissioner (SCC) was appointed to provide advice and information to all the operators and users of surveillance camera systems on the proportionate application of any new surveillance technology. Similarly, the Data Protection Act 2018, which implements the General Data Protection Regulation (GDPR), affirms that the processing of sensitive personal data, including biometrics, must be strictly necessary for the law enforcement purpose, with the Information Commissioner's Office (ICO) responsible for upholding information rights in the public interests. For the ICO, "overt, clear, and well displayed" processing information and signage is required in the absence of consent on each deployment occasion by each individual. [25] The final and central element is the police's own governance structure both on the national level, including the National Police Chief Council (NPCC), and on the local level, including the Chief Constables, the elected police and crime commissioners, and external advisory bodies such as the London Policing Ethics Panel.[26] The police also agree that consent, while it could remain implicit on the societal level, requires a strong justification in terms of necessity and proportionality, as they rely on common law rather than any specific piece of legislation permitting them to use the technology. Therefore, stakeholder trust is also conditional and conferred by the procedural requirement of justification. The overall governance

[25] Information Commissioner Office, "ICO investigation into how the police use facial recognition technology in public places," (October 31, 2019), 25. Accessed September 19, https://ico.org.uk/media/about-the-ico/documents/2616185/live-frt-law-enforcement-report-20191031.pdf.

[26] Metropolitan Police Service, "MPS LFP Guidance Document: Guidance for the MPS Deployment of Live Facial Recognition Technology," (January 24, 2020), 20. Accessed September 18, 2020, https://www.met.police.uk/SysSiteAssets/media/downloads/force-content/met/advice/lfr/mpf-lfr-guidance-document-v1-0.pdf.

structure is to ensure the well-functioning of that procedure so that trust is only conferred to the trustworthy, proving to be well-placed.

Under the current governance landscape, however, the police have a great margin of self-governance. A Parliamentary committee report observed that the Home Office's role in coordinating police policy has been significantly diminished in recent years, especially with regard to new technology.[27] The police are asked to consider the potential impacts of AFR systems upon privacy and other human rights, complete risk assessments, and provide a transparent account of what they have done, which would be available to independent and knowledgeable regulators such as the SCC and the ICO, enabling these to 'grade their homework'. However, the SCC can only encourage compliance with the Code of Practice but has no enforcement or inspection powers.[28] While the ICO may exercise statutory powers to audit and to enforce compliance, it is not clear that it could mandate the police to undertake a data protection impact assessment.[29] The guidance issued jointly by the two regulators is that they will make suggestions in response to the police's requests for advice but will not direct. Therefore, the police could choose an impact assessment template or any other alternative that they consider satisfies legal

[27] UK Parliament, "The role of the Home Office and allocation of responsibilities," (October 25, 2018). Accessed October 4, 2020, https://publications.parliament.uk/pa/cm201719/cmselect/cmhaff/515/51513.htm.

[28] Home Office, "Surveillance Camera Code of Practice," 22.

[29] House of Commons, "Facial Recognition and the Biometrics Strategy," (May 1, 2019). Accessed September 18, 2020, https://hansard.parliament.uk/commons/2019-05-01/debates/16A45B3A-6F02-4542-B5F5-2146CA0C6AB8/FacialRecognitionAndTheBiometricsStrategy.

obligations.[30] According to the regulatory guidance, the availability of technological capabilities is not in itself a justification of necessity and proportionality and that justification would need to balance the contribution of AFR systems over other policing techniques in both their effectiveness and intrusiveness for achieving the legitimate aim.[31] Nevertheless, there is no specific guidance on what would suffice as a justification and nor is there, as illustrated later, no shared consensus among stakeholders.

It is important to distinguish two groups being required to place trust. On the one hand, the public, faced by constraints on their time, know-how and resources, may readily place trust in the police's use of AFR systems, insofar as they perceive that everything is in order in the system of governance and that safeguards are in place. On the other hand, informed stakeholders with a specific interest in technology, who are in a sense embodying those safeguards and scrutinizing the AFR systems on behalf of society, may not place trust without a deliberate, analytical, and consciously effortful way of reasoning. Together, the two would jointly constitute well-placed societal trust.

[30] Surveillance Camera Commissioner and Information Commissioner Office, "Data protection impact assessments: guidance for carrying out a data protection impact assessment on surveillance camera systems," (March 18, 2020), 2. Accessed September 20, 2020, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/881538/SCC___ICO_DPIA_guidance_V3_FINAL_PDF.pdf.

[31] Surveillance Camera Commissioner, "The Police Use of Automated Facial Recognition Technology with Surveillance Camera Systems: Section 33 Protection of Freedoms Act 2012," (March 2019). Accessed September 20, 2020, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/786392/AFR_police_guidance_of_PoFA_V1_March_2019.pdf.

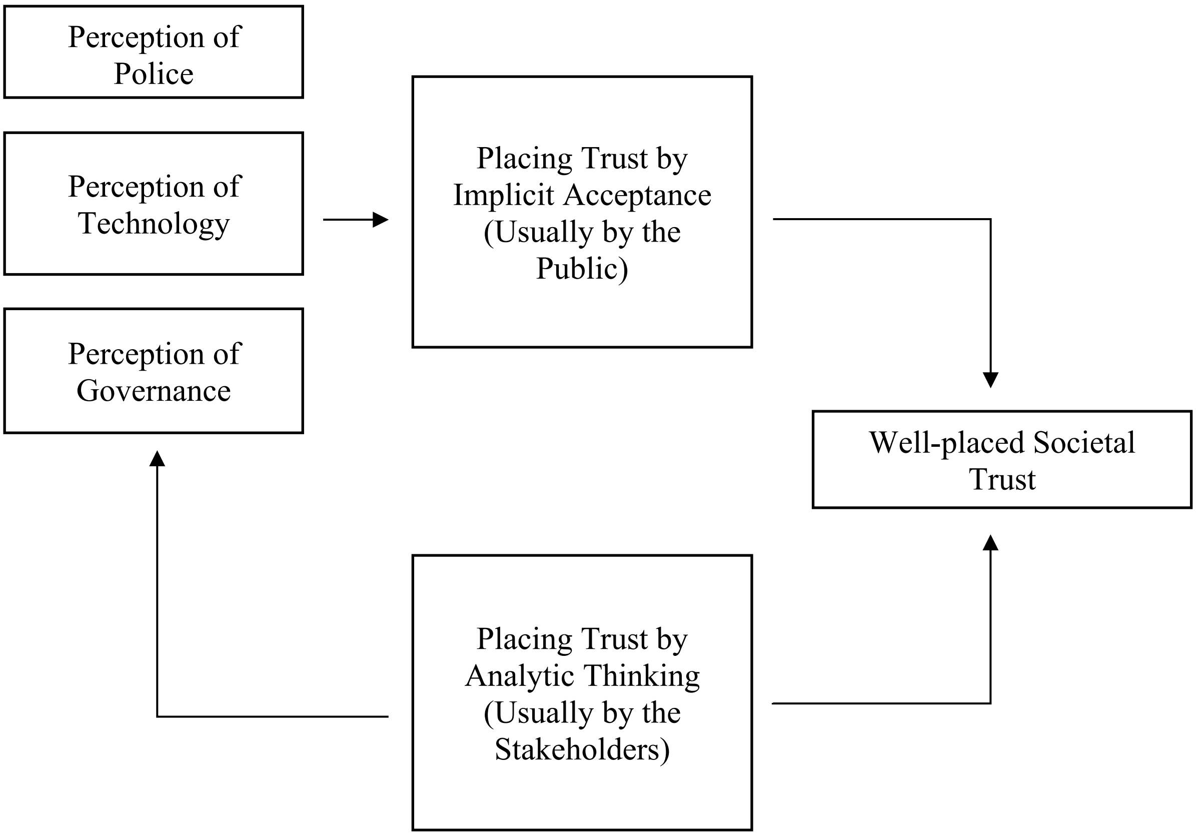
Perception of Police
Perception of Technology
Perception of Governance
Placing Trust by Implicit Acceptance (Usually by the Public)
Well-placed Societal Trust
Placing Trust by Analytic Thinking (Usually by the Stakeholders)

Figure 1: Components of Well-placed Societal Trust

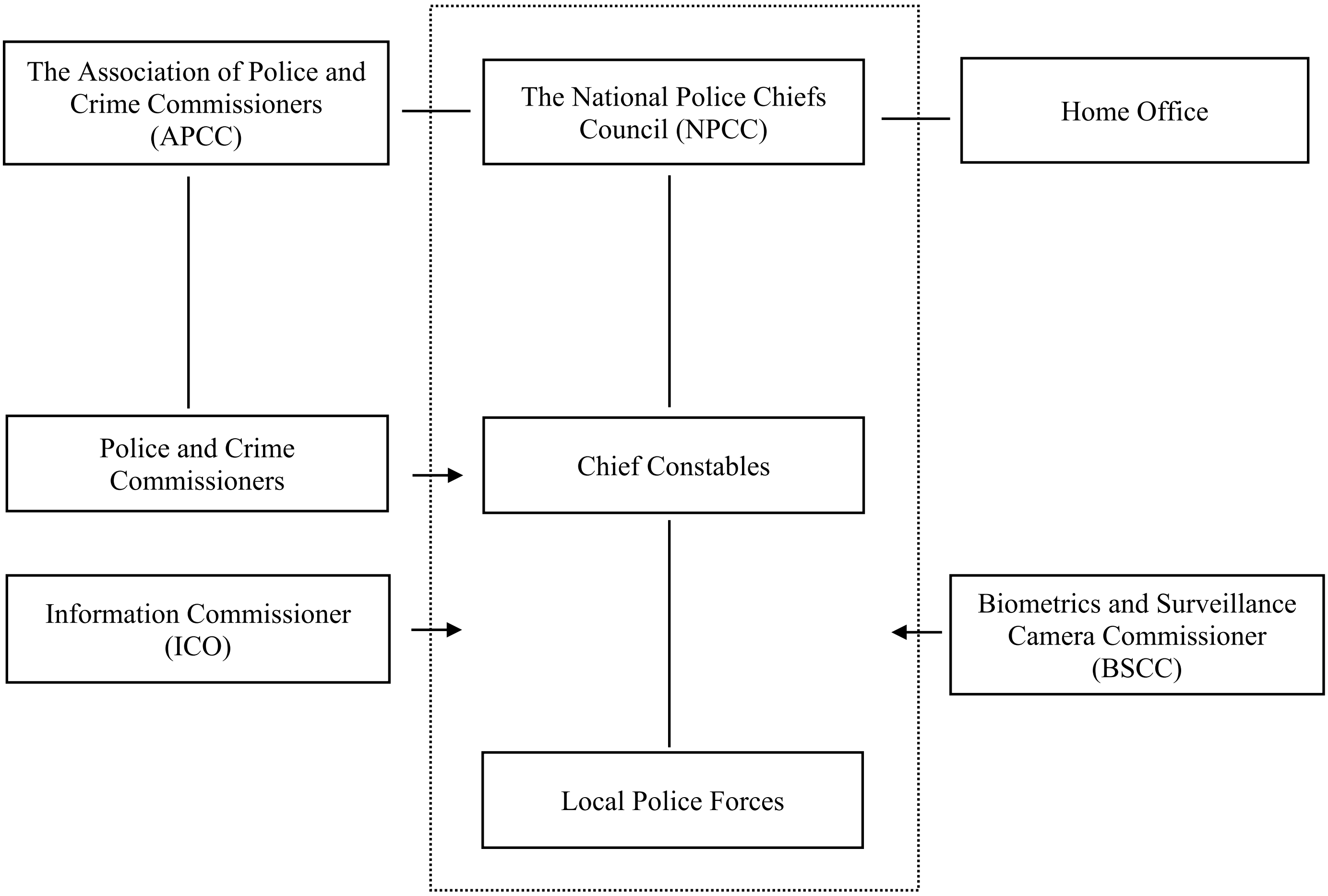
The Association of Police and Crime Commissioners (APCC)
The National Police Chiefs Council (NPCC)
Home Office
Police and Crime Commissioners
Chief Constables
Information Commissioner (ICO)
Biometrics and Surveillance Camera Commissioner (BSCC)
Local Police Forces

Figure 2: Current Governance Landscape for the Police's use of AFR systems

Note: Dash rectangle denote the police's governance structure. Horizontally, solid lines denote the collaborative relationship between participants in the regulatory space, whereas solid arrows denote the overseeing power. Vertically, solid lines denote hierarchical relationship. The figure, however, does not fully reflect the complexity of participants' relationship. For example, Law Enforcement Facial Images and New Biometrics Oversight and Advisory Board involve the Home Office, the police, and independent regulators in a collaborative way.

METHODOLOGY

This section explains the research methodology, specifically how data were collected and analyzed. I make a distinction between public trust and stakeholder trust. To understand how the stakeholders decide to place trust in the police's use of AFR systems, I carried out semi-structured interviews online with 23 stakeholders from August to September 2020: 5 interviewees are from the Government or the Parliament, 7 interviewees from academia, 7 interviewees from civil society, 3 interviewees from industry, and 1 from the police (Table 1). I adopted a sampling strategy to maximize the diversity of expert perspectives based on sectors and affiliations. I approached organizations that have been working on AFR systems or are experienced in policy and ethics of other data-driven technologies through their online presence and their involvement in policy-making process in the UK.

This sample suffers from the limitation that the police are underrepresented and I have predominantly treated the police as a unified voice. However, in reality, there may be substantive differences among different police forces and among police officers at different senior levels in their attitudes towards the AFR systems. It is also a feature of this methodology that small samples cannot be fully representative; in particular, Black, Asian, and Ethnic Minorities (BAME) communities and women are underrepresented in the sample.

The interview protocols were drafted to investigate the governance of AFR systems in general, which include both public and private sectors. The first few interviews made clear the importance of differentiating between different use cases when designing a governance framework, based on who is using the technology, what it is used for, and how it is used.[32] As this proved to be the consensus among the interviewees, I narrowed the scope of discussions to the police's overt use of live AFR systems in England and Wales. I analyzed the interview data by observing systematic agreement and disagreement among stakeholders on who should evaluate the AFR systems and by what standards.[33] To complement the interviews, I drew extensively from government and police policy documents as well as legal documents. Finally, I explored the interaction between stakeholder trust and public trust by comparing public surveys with stakeholders' observations in the interviews.

[32] Author's interviews, nos. 2, 4, 5, 8, 10, 11, 12, 13, 14, 16, 17, 18, 19, 20, 21, 22, 23, online, 2020.

[33] I initially summarized and coded each interviews manually, then using Nvivo.

Table 1: Summary of Interviewee Information

No.	Affiliation	Background
1	University of Northumbria	Academia
2	Anonymized	Industry
3	Anonymized	Academia
4	PwC	Industry
5	Anonymized	Industry
6	Independent researcher	Civil Society
7	Religious institution	Civil Society
8	Surveillance Commissioner’s Office	Government or Parliament
9	Anonymized	Academia
10	Ada Lovelace Institute	Civil Society
11	Anonymized	Government or Parliament
12	Future of Privacy Forum	Civil Society
13	House of Lords	Government or Parliament
14	Information Commissioner’s Office	Government or Parliament
15	Anonymized	Academia
16	Ada Lovelace Institute	Civil Society
17	Anonymized	Academia
18	Anonymized	Academia
19	Independent researcher	Civil Society
20	University of Cambridge	Academia
21	Local Police Force	Police
22	Involve	Civil Society
23	Police and Crime Commissioners	Government or Parliament

RESULTS

As noted above, for stakeholders to trust the AFR systems, there has to be sufficient evidence justifying the use of the technology and validating the placing of trust. According to interviewees, the AFR systems may be evaluated in terms of three types of standards: first, a technical one, for example how accurate it is across different demographic groups; secondly, a teleological one, how effective it is in achieving the stated purpose; thirdly, a social one, how effective it is compared to other alternatives and counterfactuals in terms of the balance of social benefits and costs. The technical evaluation serves as the prerequisite for the teleological and the teleological for the social, which is the ultimate standard of evaluation for necessity and proportionality.[34]

Analysis of the interview data indicates that, for the police forces' deployment of AFR systems in England and Wales, there might be both a lack of comprehensive stakeholder acceptance on all three dimensions and also a lack of mechanisms to accumulate relevant evidence.

On the technical level, it is yet to be proved that the AFR systems are accurate, for example across different demographic groups. Interviewees were skeptical that the AFR systems, like other data-driven systems, are unbiased unless proactively proven

[34] Author's interviews, nos. 1, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, online, 2020.

otherwise.[35] The skepticism aligns with a number of studies finding that AFR algorithms tend to exhibit lower performance capability against women and BAME demographics and with some even contesting the possibility of eliminating performance disparity through objective and scientific process, arguing that the systems are inherently social and political.[36; 37] The performance of AFR systems, first and foremost, depends on the training datasets for the technology. The precise scale, sources, and demographic composition of training data for AFR algorithms, nevertheless, are often commercially confidential, as for NeoFace Watch, the algorithm used by British police forces. Without access to the training datasets, the potentially discriminatory impacts of the AFR system on grounds such as race and gender cannot be thoroughly assessed.[38] Although an independent report from the National Institute of Standards and Technology (NIST) in the U.S. has previously identified NEC Corporation, the developer of NeoFace Watch, as supplying the most accurate one-to-many identification algorithm with almost undetectable false-positive differentials, this evaluation did not take into account image acquisition and other situational factors, and therefore could not "translate to everyday scenarios".[39]

[35] Author's interviews, nos. 1, 3, 4, 6, 10, 14, 16, 17, 18, 19, 20, 21, 22, online, 2020.

[36] J Buolamwini and T. Gebru, "Gender shades: Intersectional accuracy disparities in commercial gender classification," Proceedings of the 1st Conference on Fairness, Accountability and Transparency, PMLR 81 (2018): 77-91.

[37] Kate Crawford and Trevor Paglen, "Excavating AI: The Politics of Images in Machine Learning Training Sets," The AI Now Institute, New York University. Accessed October 22, 2020, https://www.excavating.ai/.

[38] The UK Court of Appeal, R (Bridges) -v- CC South Wales & others, para 196.

[39] Patrick Grother, Mei Ngan, and Kayee Hanaoka, "Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects", National Institute of Standards and Technology, U.S. Department of Commerce, NISTIR 8280, 9. Accessed September 14, 2020, https://doi.org/10.6028/NIST.IR.8280.

Accordingly, interviewees emphasized that technical performance of the system ought to be evaluated within specific use cases and contexts.[40] Yet, among all the different ways accuracy and non-discrimination could be measured, there are no consistent guidelines on how to evaluate AFR systems in a wide range of real-world scenarios used by the police forces. In a naturalistic environment, AFR systems are found to struggle in large crowds and low light. Furthermore, poor-quality custody images on the watchlists, relatively low similarity scores (ranging from 55% to 60%), and other case-specific configurations affect the accuracy of systems contributing to 2,755 false positive alerts out of 2900 possible matches generated by SWP's deployment of AFR system from June 2017 to March 2018.[41]

It is highly contested whether the outcomes constitute evidence for or against the accuracy of the system. The reason lies in the availability of evidence. For privacy reasons, the facial biometrics of persons are immediately and automatically deleted when no match is made, leaving the total number of all faces scanned by the AFR system during the trials, along with their ethnic and gender breakdown, unknown. Without this the number of false positive alerts as well as the comparison of numbers across demographic

[40] Author's interviews, nos. 2, 4, 5, 8, 10, 11, 12, 13, 14, 16, 17, 18, 19, 20, 21, 22, online, 2020.

[41] Bethan Davies, Martin Innes and Andrew Dawson, "An Evaluation of South Wales Police's Use of Automated Facial Recognition," (September 2018), 8 and 21. Accessed 16 July, 2020, https://static1.squarespace.com/static/51b06364e4b02de2f57fd72e/t/5bfd4fbc21c67c2cdd692fa8/1543327693640/AFR+Report+%5BDigital%5D.pdf.

groups are not available for any definitive conclusion about the technical performance of the system.[42] There are some efforts undertaken by both the police forces and independent researchers to fill this vacuum in the technical evidence. Interestingly, the police tend to evaluate accuracy by the proportion of false-positive alerts in an estimated total number of recognition opportunities, as opposed to many researchers, who focus on the proportion of false-positive alerts in the total number of alerts generated by the

[42] The UK High Court of Justice, "Skeleton Argument on Behalf of the Claimant," CO/4085/2018, para 113. Accessed December 1, 2020, https://www.libertyhumanrights.org.uk/wp-content/uploads/2020/02/Claimants-Skeleton-Argument.pdf.

AFR systems.[43] Consequently, for the same trial, the police may claim that the system is 99% accurate, while researchers may assert that more than 70% of matches are incorrect.[44] The absence of agreed standards for evaluation thus introduces conflicting evidence and misunderstandings.

Table 2: Example of Different Interpretations of Accuracy
(Statistics from the MPS's Romford Deployment, Feburary 2019)

Estimated number of recognition opportunities	7300
Number of alerts	10
Number of people engaged by a police officer following an alert	5
Number of alerts confirmed correct	3
Accuracy as Estimated False Positive Identification Rate defined by the MPS = (Number of alerts – Number of confirmed identification)/ Estimated total number of recognition opportunities	(10-3)/7300 = 0.09%
Accuracy as False Positive Match Rate[45] = (Number of alters – Number of confirmed identification)/Number of alerts	(10-3)/10 = 70%

As for evaluating the possibility of bias, the Universities' Police Science Institute (UPSI) in Cardiff has been commissioned by the SWP to test the algorithm since November

[43] In MPS's document, a recognition opportunity occurs "when a person's face is visible to an LFR camera as they move through the Zone of Recognition."See Metropolitan Police Service, "Metropolitan Police Service Live Facial Recognition Trials," (February 2020), 5. Accessed September 15, 2020, https://www.met.police.uk/SysSiteAssets/media/downloads/central/advice/met/facial-recognition/met-evaluation-report.pdf.

[44] Metropolitan Police Service, "Metropolitan Police Service Live Facial Recognition Trials," 13-15.

[45] See, for example, the definition adopted by Big Brother Watch. Big Brother Watch, "Face Off: The lawless growth of facial recognition in UK policing," (May 2018), 3. Accessed October 3, 2020, https://bigbrotherwatch.org.uk/wp-content/uploads/2018/05/Face-Off-final-digital-1.pdf.

2019.[46] However, the testing is only taking place after two-year deployment and has not yet published any result.[47] In non-operational trials conducted by the MPS and reviewed by the National Physical Laboratory (NPL) between 2016 and 2019, where the demographic details of all scanned faces were recorded, the differences in algorithm performance were found to be statistically significant (p = 10%) with respect to gender although not ethnicities.[48] However, the disparity in performance was not considered by the MPS as sufficient evidence against the use of an immature technology, as they use an improved adjudication process for human operators to mitigate the presence of bias.[49] Their assumption is that the human failsafe process should be taken into the evaluation of system performance as part of the AFR system.

Therefore, there still remain some important technical performance questions that need to be addressed carefully, as opposed to the police's claim that the testing and the piloting have "all been done".[50] Different statistical standards for fairness reflect different normative conceptions of fairness.[51] Evaluating an AFR systems involves implicit ethical decisions on what accuracy across different demographic groups entails. First, the

[46] South Wales Police, "Resources: Judicial Review Appeal FAQ", (August 2020), 3. Accessed September 14, 2020, https://afr.south-wales.police.uk/wp-content/uploads/2020/08/AFR-updated-briefing-and-QA-Aug20.docx.

[47] The testing was planned to commence since early 2020 but postponed due to COVID-19.

[48] Metropolitan Police Service, "Metropolitan Police Service Live Facial Recognition Trials," 25.

[49] Ibid, 4.

[50] BBC Radio 5 Live, "Stephen Nolan's Interview with Ken Marsh, Metropolitan Police Federation Chairman, and Dr. Stephanie Hare," (January 24, 2020).

[51] Mark MacCarthy, "Standards of Fairness for Disparate Impact Assessment of Big Data Algorithms," *Cumberland Law Review 48*, no. 1 (2017): 67-148.

evaluation may only incentivize developers to address performance disparities on the tasks they are publicly audited for. For example, while performance disparities across subgroups that have been the focus of prior public audits, such as binary gender and skin type, may consequently be reduced, a gender stereotype might simultaneously be promoted.[52] Secondly, if an algorithm is programmed to produce equal accuracy rates across groups, it will necessarily produce unequal false-positive rates.[53] What these measures imply requires further investigation to decide whether to minimize false positives or false negatives or strike a balance between them.

In terms of the teleological standard, it is still contested whether the AFR systems are effective in achieving the stated purposes. According to the SWP, AFR systems are primarily for "the prevention and detection of crime", specifically the apprehension of suspects on warrants.[54] Similarly, the MPS proclaims that AFR systems are to "help tackle serious violence" and "protect the vulnerable".[55] Despite these statements, many interviewees stated that the police had failed to clearly articulate what they were hoping to achieve and what the measures of success would be.[56] For example, the SWP's policy

[52] Inioluwa Deborah Raji, Timnit Gebru, Margaret Mitchell, Joy Buolamwini, Joonseok Lee, and Emily Denton. 2020. Saving Face: Investigating the Ethical Concerns of Facial Recognition Auditing. In Proceedings of the 2020 AAAI/ACM Conference on AI, Ethics, and Society (AIES '20), February 7–8, 2020, New York, NY, USA. ACM, New York, NY, USA, 7 pages.

[53] Emily Berman, "A Government of Laws and not of Machines," Boston University Law Review 98 (2018): 1328.

[54] South Wales Police, "Privacy Impact Assessment Version 4.0," (February 12, 2018), 3. Accessed September 15, 2020, https://afr.south-wales.police.uk/wp-content/uploads/2019/10/PIA-V4-signed.pdf.

[55] Metropolitan Police Service, "Live Facial Recognition." Accessed September 15, 2020, https://www.met.police.uk/advice/advice-and-information/facial-recognition/live-facial-recognition/.

[56] Author's interviews, nos. 3, 6, 8, 9, 10, 13, 15, online, 2020.

documents give little guidance on the composition of their watchlist and the location of AFR deployment, allowing any person "where intelligence is required" to be placed on a watchlist "in all event types".[57; 58] The range is without apparent limits and leaves vague what the AFR systems would be used for. The ICO has echoed interviewees' opinions and considered the SWP's deployments insufficiently informed by intelligence and without a specific objective.[59]

Moreover, a few interviewees argued that the police's trial methodology was problematic because it focused primarily on the technical aspects of the trials, such as accuracy of matching, but was less clear on how the test deployments were intended to achieve the non-technical aspects, or in other words the utility of AFR systems as a policing tool.[60; 61] In their applications for funding to the Home Office Police Transformation Fund, the SWP detailed "decreases in repeat offending" and "savings related to reduced investigation and prosecution time" as intended outcomes from the use of AFR systems.[62] Nevertheless, there is no evidence illustrating whether these outcomes were met, with the academic

[57] South Wales Police, "Privacy Impact Assessment Version 4.0," (February 12, 2018), para 1.9.

[58] South Wales Police, "Data Protection Impact Assessment," (October 21, 2018), 20. Accessed September 15, 2020, https://afr.south-wales.police.uk/wp-content/uploads/sites/4/2020/05/DPIA-V5.4-Live.pdf.

[59] Information Commissioner Office, "ICO investigation into how the police use facial recognition technology in public places," 22.

[60] Author's interviews, nos. 1, 6, 14, 16, online, 2020.

[61] Peter Fussey and Daragh Murray, "Independent Report on the London Metropolitan Police Service's Trial of Live Facial Recognition Technology," Project Report, University of Essex Human Rights Centre (2019): 7.

[62] Information Commissioner Office, "ICO investigation into how the police use facial recognition technology in public places," 8.

evaluation commissioned by the SWP only in its preliminary stage.[63] The MPS indeed reported that following alerts from the AFR systems and police officers' adjudication of the alerts, during the operational trials, 30% of interventions resulted in an arrest, compared to a 13% arrest rate from the alternative stop and search tactic, citing the comparison as the evidence for the utility of AFR systems as a policing tool. [64] Nevertheless, it may be challenged whether the arrest rates reported by the police themselves constitute as sufficient evidence in supportive of effectiveness. Many interviewees acknowledged that the police do know more details, welcoming practical understandings grounded in daily experience.[65] However, some interviewees cautioned against confirmation bias and technological solutionism that might convince the police to be inclined to believe any indication that the technology will make it easier for them to 'get the bad guys.' [66]

In terms of meeting the need for social benefit, it is still to be properly assessed whether the AFR systems are effective and proportionate in a democratic society. Although the courts to date have consistently upheld the judgement that the SWP's deployment was proportional, or that the appropriate balance had been stricken between the infringement of the privacy rights of individuals and the interests of society, interviewees

[63] Author's phone call with an anonymous informant from Universities' Police Science Institute of Cardiff University, London, 2020.

[64] Metropolitan Police Service, "Metropolitan Police Service Live Facial Recognition Trials," 4.

[65] Author's interviews, nos. 3, 4, 8, 9, 11, 15, 17, 18, 21, online, 2020.

[66] Author's interviews, nos. 1, 3, 4, 6, 9, 18, 23, online, 2020.

agreed that it should not be for the courts to adjudicate this but rather should be a matter of public debate.[67] This is to ask: do 'we' really want to live in a society with the AFR systems operating like this? The current legal framework as the shared consensus of the democratic society is seen as impotent to provide a full answer to the question, for the AFR systems are framed as a fundamentally different form of policing and surveillance that disrupts the previous consensus. Therefore, a social evaluation of the technology is seen as a renegotiation of consent to its use, which, for interviewees, either 'has not happened yet' or 'is ongoing'. Interviewees pointed to open-ended public surveys, civil society activism, citizen councils, and most frequently mentioned, a parliamentary debate as a plurality of appropriate forms of societal discussion. Because there is 'no one set of public opinion to be found', many interviewees recommended that these forms of discussion should all proceed, taking into account both majority and minority opinions, for their reaction to the past trials and their visions for the future, inclusive of demographic, geographic or other communities of all kinds.[68]

Many interviewees expressed concern about the long-term impacts of the AFR systems upon local communities and their way of life.[69] Although the MPS has tried to argue for the social value of AFR systems by contrasting them with other policing tactics in terms of the number of arrests and financial investment, it makes no mention of the potential

[67] Author's interviews, nos. 1, 2, 3, 4, 6, 10, 13, 15, 16, 19, 22, 23, online, 2020.

[68] Author's interviews, nos. 1, 6, 9, 12, 17, 18, 19, 21, 22, online, 2020.

[69] Author's interviews, nos. 1, 3, 6, 7, 13, 14, 15, 19, online, 2020.

indirect effects of using the technology.[70] Behind the MPS's argument is the assumption that evidence for teleological effectiveness is in itself evidence for social effectiveness, an assumption that is also reflected in the comments from the MPS Commissioner, Britain's most senior police officer, who stated that critics, rather than the police, shoulder the burden of proof on why the police should not be allowed to use AFR systems to fight violent crimes.[71] Nevertheless, even if working perfectly, the AFR systems may reinforce the transformation the relationship between citizens and the state started by the ubiquity of CCTV, abandoning the presumption of innocence and treating everyone as a potential suspect.[72] If so, the AFR systems could discourage political participation, known as the 'chilling effect', and jeopardize a democratic fundamental.[73] Therefore, a few interviewees emphasized the imperative to involve sociologists, anthropologists, criminologists, economists, psychologists, and Science, Technology, Society scholars, experts who study how society operates and what the role of technology is, in the social evaluation of the AFR systems.[74]

[70] Metropolitan Police Service, "Live Facial Recognition: Legal Mandate," 14. Accessed September 21, 2020, https://www.met.police.uk/SysSiteAssets/media/downloads/force-content/met/advice/lfr/mps-lfr-legal-mandate-v1-1.pdf.

[71] Martin Evans, "Met Chief defends facial recognition technology as vital tool in fight against violent crime," *The Telegraph* (February 24, 2020). Accessed September 22, 2020, https://www.telegraph.co.uk/news/2020/02/24/met-chief-defends-facial-recognition-technology-vital-tool-fight/.

[72] Author's interviews, nos. 6, 7, 19, online, 2020.

[73] Author's interviews, nos. 3, 17, online, 2020.

[74] Author's interviews, nos. 4, 9, 15, online, 2020.

What further complicates the social evaluation of the AFR systems is the continuous interaction between technology and society. As the cultural history of CCTV unfolds, the social costs of eroding privacy and a trusting relationship between citizens and the state would depend upon people's early encounters with the technology.[75] Positive encounters with technology render it less intrusive and reproduce trust. As previously discussed, most of the public think that appropriate safeguards and restrictions are the prerequisites for permitting the police's use of AFR systems for law enforcement purposes.[76] With the Court of Appeal ruling that the legal framework regulating the police's use of AFR systems is insufficient and the overwhelming majority of interviewed stakeholders arriving at the same conclusion, it may be reasonable to speculate that the social costs would inflate if the police continue to deploy the AFR systems without governance safeguards clearly demonstrated to the public.

The reform or re-negotiation most interviewees had in mind, however, is not to propose a new piece of primary legislation, because they considered the existing principle-based one to be adequate, but to develop secondary legislation, similar to the Surveillance Camera Code of Practice, to guide the evaluation of proportionality for different use cases of AFR systems specifically.[77] Because the potential effects of the technology remain largely unknown, interviewees also emphasized that evaluation should be periodic, not

[75] Adam Thierer, "A Framework for Benefit-Cost Analysis in Digital Privacy Debates," George Mason Law Review 20, no. 4 (2013): 1055-1105.

[76] Ada Lovelace Institute, "Beyond face value: public attitudes to facial recognition technology," 8.

[77] Author's interviews, nos. 8, 9, 11, 13, 14, 15, 16, 17, 18, 21, 23, online, 2020.

one-time.[78] Interviewees agreed on a layered, co-governance approach: with sectoral knowledge and grounded experience, the police should clearly articulate the purpose for which the AFR systems are used and demonstrate their effectiveness in achieving the stated purpose; however, independent regulators, such as the Information Commissioner and the newly combined Surveillance Camera and Biometrics Commissioner, [79] should be entrusted with statutory enforcement powers, ‘the teeth’, to audit and veto the use of the AFR systems. Not only would independent regulators provide safeguards against confirmation bias, but they also integrate a broader variety of perspectives from society. The co-governance framework would serve to experiment and gather evidence on the behalf of society as a whole. Such governance approach requires granting the existing regulators more power and funding as well as a clearer delineation of their jurisdiction. The recent ruling by the Court may open a timely policy window to do so. Nevertheless, several interviewees insisted on the necessity of developing a new piece of primary legislation debated through the Parliament,[80] as the only legitimate place a democratic society may resort to when consensus is broken, to consider the necessity and proportionality question for different use cases of AFR systems – not only for the public sector but also for the private one, which, almost all interviewees agree, is under even less public scrutiny.[81]

[78] Author’s interviews, nos. 2, 14, 15, online, 2020.

[79] HM Government Public Appointments, “Biometrics and Surveillance Camera Commissioner,” (July 9, 2020). Accessed September 22, 2020. https://publicappointments.cabinetoffice.gov.uk/appointment/biometrics-and-surveillance-camera-commissioner/.

[80] Author’s interviews, 2, 3, 6, 7, 10, 19, online, 2020.

[81] Author’s interviews, 1, 2, 3, 4, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, online, 2020.

While stakeholders define whether societal trust is well-placed, stakeholder trust is insufficient for well-placed societal trust in AFR systems. After all, the public too must come to trust the use of the technology. To inform the public, the MPS put signage advertising the presence of AFR cameras, marked the vans used as control centers for the AFR deployment, and published policy documents such as the legal mandate and the data protection impact assessment online. Nevertheless, transparency does not necessarily ensure that the information placed in the public domain is, in practice, accessible and in fact accessed. Interviewees' observations align with the survey data, suggesting that the public are likely to place trust in a general manner, even with little or no knowledge about the AFR systems. Nevertheless, interviewees drew attention to three ways in which such the public's intuitive way of placing trust may actually cultivate public distrust in today's contexts: first, people may be informed through media with 'dramatic headlines', which is hardly conducive to a good understanding of the technology and its use in reality;[82] secondly, people may understand technology by 'dumping everything together', with an imagery of AFR systems as the surveillance tool by the state having spill-over effects and eroding public trust in other use cases; [83] thirdly, people may be confused by inconsistent policies from the 43 police forces, if each of them decide to do things noticeably differently in absence of a national strategy.[84]

[82] Author's interviews, nos. 5, 12, 13, 15, 21, online, 2020.

[83] Author's interviews, nos. 5, 12, online, 2020.

[84] Author's interviews, nos. 1, 4, 10, 12, 14, 17, 19, 21, online, 2020.

Therefore, there is not only a role for public input in evaluating the social benefits and costs of the AFR systems but also one for public communication in facilitating better understanding of the technology among the public. The information flow among the public, regulators, and the police should be interactive. Convened by the Ada Lovelace Institute and only halfway through the process, the Citizens' Biometrics Council was identified by many interviewees as a paradigm for guiding small groups of the public through controversial scenarios, dilemmas, and trade-offs to enable deliberation and mutual understanding.[85; 86] The paradigm challenges the distinction between the public and stakeholders that emerged in the above analysis: the distinction may be true at present, but will not necessarily remain true and perhaps should be proactively remedied in the future.

[85] Ada Lovelace Institute, "No green lights, no red lines: Public perspectives on COVID-19 technologies," (July 2020). Accessed 16 July, 2020, https://www.adalovelaceinstitute.org/wp-content/uploads/2020/07/No-green-lights-no-red-lines-final.pdf.

[86] Author's interviews, nos. 1, 5, 10, 13, 16, online, 2020.

CONCLUSION

For the society to trust an innovative technology and for this trust to be well-placed, a good governance framework must ensure both public trust and stakeholder trust. On the one hand, the public place trust in the use of the technology embedded in broader socio-technical systems heuristically, therefore determining whether there is societal trust. On the other hand, stakeholders place trust deliberatively and look for evidence justifying the use, therefore determining whether such societal trust is well-placed.

For the police's deployment of the AFR systems in the England and Wales, the cultural history of policing by consent may have readily extended public trust to innovative ways of policing, whereas the existing data protection governance have both defined 'necessity and proportionality' as justification and left considerable space for divergent interpretations of the phrase among stakeholders. Drawing from 23 stakeholder interviews and documentary materials, this essay argues that the accumulation of evidence has not contributed to more understanding on AFR systems across three levels of evaluation—the technical, the teleological, and the social. Indeed, there are at times distinctive and often conflicting assumptions, noticeably between the police and other stakeholders, on how to interpret evidence and who can do so authoritatively. The lack of stakeholder trust warns against licensing the police's use of AFR systems, despite high public trust, because public trust may be mistaken. Furthermore, the lack of stakeholder trust is likely to eventually contribute to the public's negative perception of AFR systems and erode public trust.

Therefore, a layered co-governance framework that effectively coordinates grounded experience from the police, expertise from social scientists, and deliberate perspectives from the public is urgently needed. While the UK government is reviewing the governance framework and considering its simplification and extension, it should do so fast enough to keep up with the diffusion of the technology to maintain public trust and fulfil its own vision.[87]

[87] Home Office, "Home Office in the media blog: Monday 17 June," (June 17, 2019). Accessed September 21, 2020, https://homeofficemedia.blog.gov.uk/2019/06/17/home-office-in-the-media-blog-monday-17-june/.

APPENDIX

Draft Semi-structured Interview Protocols

1. **Overview**

   1. What are the key issues in setting up a regulatory framework for AFR systems?

2. **Thinking about Standards**

   2. Who should evaluate the AFR systems?

   3. What should be the standards for evaluation?

3. **Enforcing Standards**

   4. Are current accountability mechanisms the police's use of AFR adequate?

   5. Are current accountability mechanisms for private sector's use of AFR adequate? For example, in shopping centres?

4. **Trust**

   6. What might enhance public trust in the use of AFR systems?

   7. Anything you would like to add that we have not talked about, but you think important and helpful to do some research on?

BIBLIOGRAPHY

Ada Lovelace Institute. “Beyond face value: public attitudes to facial recognition technology.” September 2019. Accessed September 18, 2020, https://www.adalovelaceinstitute.org/wp-content/uploads/2019/09/Public-attitudes-to-facial-recognition-technology_v.FINAL_.pdf.

Ada Lovelace Institute. “No green lights, no red lines: Public perspectives on COVID-19 technologies.” July 2020. Accessed July 16, 2020, https://www.adalovelaceinstitute.org/wp-content/uploads/2020/07/No-green-lights-no-red-lines-final.pdf.

BBC Radio 5 Live. “Stephen Nolan’s Interview with Ken Marsh, Metropolitan Police Federation Chairman, and Dr. Stephanie Hare.” January 24, 2020.

Berman, E. “A Government of Laws and not of Machines.” *Boston University Law Review 98* (2018).

Big Brother Watch. “Face Off: The lawless growth of facial recognition in UK policing.” May 2018. Accessed October 3, 2020, https://bigbrotherwatch.org.uk/wp-content/uploads/2018/05/Face-Off-final-digital-1.pdf.

BMG Research. “Public Perception of Policing in England and Wales 2018.” January 2019. Accessed September 16, 2020, https://www.bmgresearch.co.uk/wp-content/uploads/2019/01/1578-HMICFRS-Public-Perceptions-of-Policing-2018_FINAL.pdf.

Brown, D. and Quinton, Paul. “Integrity Programme: Data pack on public trust and confidence in the police.” College of Policing.” Accessed September 16, 2020, https://www.college.police.uk/What-we-do/Ethics/Documents/Data_pack_Public_trust.pdf.

Buolamwini J. and Gebru, T. “Gender shades: Intersectional accuracy disparities in commercial gender classification.” Proceedings of the 1st Conference on Fairness, Accountability and Transparency, PMLR 81 (2018): 77-91.

Crawford, K. and Paglen, T. “Excavating AI: The Politics of Images in Machine Learning Training Sets,” The AI Now Institute, New York University. Accessed October 22, 2020, http://www.excavating.ai/.

Davies, B., Innes, M., and Dawson, A. “An Evaluation of South Wales Police’s Use of Automated Facial Recognition.” September 2018. Accessed July 16, 2020, https://static1.squarespace.com/static/51b06364e4b02de2f57fd72e/t/5bfd4fbc21c67c2cdd692fa8/1543327693640/AFR+Report+%5BDigital%5D.pdf.

Emsley, Clive. *The English Police: A Political and Social History*. London: Routledge, 1997.

Evans, Martin. “Met Chief defends facial recognition technology as vital tool in fight against violent crime.” *The Telegraph*. February 24, 2020. Accessed September 22, 2020, https://www.telegraph.co.uk/news/2020/02/24/met-chief-defends-facial-recognition-technology-vital-tool-fight/.

Fussey P. and Murray, D. “Independent Report on the London Metropolitan Police Service’s Trial of Live Facial Recognition Technology.” Project Report, University of Essex Human Rights Centre. 2019.

Grother, P., Ngan, M., and Hanaoka, K. “Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects.” National Institute of Standards and Technology, U.S. Department of Commerce, NISTIR 8280. Accessed September 14, 2020, https://doi.org/10.6028/NIST.IR.8280.

Hardin, Russell. *Trust.* Cambridge: Polity Press, 2006.

Hintz, Arne. “The politics of surveillance policy: UK regulatory dynamics after Snowden,” *Internet Policy Review 5*, no. 3 (September 2016): 1-16. DOI: 10.14763/2016.3.424.

HM Government Public Appointments. “Biometrics and Surveillance Camera Commissioner.” July 9, 2020. Accessed September 22, 2020, https://publicappointments.cabinetoffice.gov.uk/appointment/biometrics-and-surveillance-camera-commissioner/.

Home Office. “Biometrics Strategy: Better public services and Maintaining public trust.” June 2018, 13. Accessed September 19, 2020, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/720850/Home_Office_Biometrics_Strategy_-_2018-06-28.pdf.

Home Office. “FOL release: Definition of policing by consent.” December 10, 2012. Accessed September 16, 2020, https://www.gov.uk/government/publications/policing-by-consent/definition-of-policing-by-consent.

Home Office. “Home Office in the media blog: Monday 17 June.” June 17, 2019. Accessed September 21, 2020, https://homeofficemedia.blog.gov.uk/2019/06/17/home-office-in-the-media-blog-monday-17-june/.

Home Office. “Surveillance Camera Code of Practice.” June 2013. Accessed September 16, 2020, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/282774/SurveillanceCameraCodePractice.pdf.

House of Commons. “Facial Recognition and the Biometrics Strategy.” May 1, 2019. Accessed September 18, 2020, https://hansard.parliament.uk/commons/2019-05-01/debates/16A45B3A-6F02-4542-B5F5-2146CA0C6AB8/FacialRecognitionAndTheBiometricsStrategy.

Information Commissioner Office. “ICO investigation into how the police use facial recognition technology in public places.” October 31, 2019. Accessed September 19, https://ico.org.uk/media/about-the-ico/documents/2616185/live-frt-law-enforcement-report-20191031.pdf.

Jackson, J., Hough, M., Bradford, B., Katrin, H., and Kuha, J. “Policing by consent: understanding the dynamics of police power and legitimacy.” *ESS country specific topline results series 1*. 2012. European Commission. Accessed September 19, 2020, http://eprints.lse.ac.uk/47220/1/Policing%20by%20consent(lsero).pdf.

Jobin, A., Ienca, M., and Vayena, E. “The global landscape of AI ethics guidelines.” *Nat Mach Intell 1* (2019): 389–399.

Kroener, Inga. “CCTV: A technology under the radar?” PhD Thesis, University College London. 2009. Accessed September 22, 2020, https://discovery.ucl.ac.uk/id/eprint/19711/1/19711.pdf.

London Policing Ethics Panel. “Final Report on Live Facial Recognition.” May 2019. Accessed September 19, 2020, http://www.policingethicspanel.london/uploads/4/4/0/7/44076193/live_facial_recognition_final_report_may_2019.pdf.

MacCarthy, Mark. "Standards of Fairness for Disparate Impact Assessment of Big Data Algorithms." *Cumberland Law Review 48*, no. 1 (2017): 67-148.

Metropolitan Police Service. “Live Facial Recognition: Legal Mandate.” Accessed September 21, 2020, https://www.met.police.uk/SysSiteAssets/media/downloads/force-content/met/advice/lfr/mps-lfr-legal-mandate-v1-1.pdf.

Metropolitan Police Service. “Live Facial Recognition.” Accessed September 15, 2020, https://www.met.police.uk/advice/advice-and-information/facial-recognition/live-facial-recognition/.

Metropolitan Police Service. “Metropolitan Police Service Live Facial Recognition Trials.” February 2020. Accessed September 15, 2020, https://www.met.police.uk/SysSiteAssets/media/downloads/central/advice/met/facial-recognition/met-evaluation-report.pdf.

Metropolitan Police Service. “MPS LFP Guidance Document: Guidance for the MPS Deployment of Live Facial Recognition Technology.” January 24, 2020. Accessed September 18, 2020, https://www.met.police.uk/SysSiteAssets/media/downloads/force-content/met/advice/lfr/mpf-lfr-guidance-document-v1-0.pdf.

Norris, Clive. “The success of failure. Accounting for the global growth of CCTV.” In *Routledge Handbook of Surveillance Studies*, ed. Kirstie Ball, Kevin D. Haggerty, and David Lyon, 251-258. London: Routledge, 2014.

O’Neill, Onora. “Linking Trust to Trustworthiness.” *International Journal of Philosophical Studies 26*, no. 2 (2018).

O’Neill, Onora. *A Question of Trust: The BBC Reith Lectures 2002*. Cambridge: Cambridge University Press, 2002.

Open Data Institute. “Designing trustworthy data institutions.” 2020. Accessed September 26, 2020, http://theodi.org/wp-content/uploads/2020/04/OPEN_Designing-trustworthy-data-institutions_ODI_2020.pdf.

Pettit, Philip. “The cunning of trust.” *Philosophy & Public Affairs 24*, no. 3 (1995): 202-225.

Police Service of Northern Ireland. “Freedom of Information Request: F-2020-00188.” Accessed November 1, 2020, https://www.psni.police.uk/globalassets/advice--information/our-publications/disclosure-logs/2020/organisational-informal-and-governance/00188-facial-recognition-technology.pdf.

Raji, I. D., Gebru, T., Mitchell, M., Buolamwini, J., Lee, J., and Denton, E. 2020. Saving Face: Investigating the Ethical Concerns of Facial Recognition Auditing. In Proceedings of the 2020 AAAI/ACM Conference on AI, Ethics, and Society (AIES ’20). February 7–8, 2020, New York, NY, USA.

South Wales Police. “Data Protection Impact Assessment.” October 21, 2018. Accessed September 15, 2020, https://afr.south-wales.police.uk/wp-content/uploads/sites/4/2020/05/DPIA-V5.4-Live.pdf.

South Wales Police. “Privacy Impact Assessment Version 4.0.” February 12, 2018. Accessed September 15, 2020, https://afr.south-wales.police.uk/wp-content/uploads/2019/10/PIA-V4-signed.pdf.

South Wales Police. “Resources: Judicial Review Appeal FAQ.” August 2020. Accessed September 14, 2020, https://afr.south-wales.police.uk/wp-content/uploads/2020/08/AFR-updated-briefing-and-QA-Aug20.docx.

Spriggs, A., Argomaniz, J., Gill, M., and Bryan, J. “Public attitudes towards CCTV: results from the Pre-intervention Public Attitude Survey carried out in areas implementing CCTV,” Home Office Online Report 10/15. 2005. Accessed September 16, 2020, http://library.college.police.uk/docs/hordsolr/rdsolr1005.pdf.

Surveillance Camera Commissioner and Information Commissioner Office. “Data protection impact assessments: guidance for carrying out a data protection impact assessment on surveillance camera systems.” March 18, 2020. Accessed September 20, 2020, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/881538/SCC___ICO_DPIA_guidance_V3_FINAL_PDF.pdf.

Scottish Parliament. “Facial Recognition: How Policing in Scotland Makes Use of This Technology.” Accessed November 1, 2020, https://digitalpublications.parliament.scot/Committees/Report/JSP/2020/2/11/Facial-recognition--how-policing-in-Scotland-makes-use-of-this-technology.

Surveillance Camera Commissioner. “The Police Use of Automated Facial Recognition Technology with Surveillance Camera Systems: Section 33 Protection of Freedoms Act 2012.” March 2019. Accessed September 20, 2020, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/786392/AFR_police_guidance_of_PoFA_V1_March_2019.pdf.

Thierer, Adam. “A Framework for Benefit-Cost Analysis in Digital Privacy Debates,” *George Mason Law Review 20*, no. 4 (2013): 1055-1105.

UK Court of Appeal. *R (Bridges) -v- CC South Wales & others*.

UK Government. “Confidence in the local police.” March 4, 2020. Accessed September 16, 2020, https://www.ethnicity-facts-figures.service.gov.uk/crime-justice-and-the-law/policing/confidence-in-the-local-police/latest#by-ethnicity-over-time.

UK High Court of Justice. “Skeleton Argument on Behalf of the Claimant.” CO/4085/2018. Accessed December 1, 2020, https://www.libertyhumanrights.org.uk/wp-content/uploads/2020/02/Claimants-Skeleton-Argument.pdf.

UK Parliament. “The role of the Home Office and allocation of responsibilities.” October 25, 2018. Accessed October 4, 2020,https://publications.parliament.uk/pa/cm201719/cmselect/cmhaff/515/51513.htm.

UNIVERSITY OF CAMBRIDGE

Bennett Institute for Public Policy Cambridge

www.bennettinstitute.cam.ac.uk