



HOUSE OF LORDS

House of Lords  
London  
SW1A 0PW

[HLJusticeHomeAffairs@parliament.uk](mailto:HLJusticeHomeAffairs@parliament.uk)  
[www.parliament.uk/lords](http://www.parliament.uk/lords)

Rt. Hon. James Cleverly MP  
Home Secretary  
Home Office  
2 Marsham Street  
London SW1P 4DF

26 January 2024

Dear Home Secretary,

1. The Justice and Home Affairs Committee is investigating the use of Live Facial Recognition (LFR) Technology by police forces in England and Wales. We set out our key findings in the Appendix to this letter. We draw to your particular attention:
  - **The absence of a foundation in law for the deployment of LFR (see Appendix, paragraphs 1–5)**
  - **The lack of clear standards and regulation in respect of the use of LFR**
  - **The importance of consistent approaches to training in the use of LFR by police forces in England and Wales**

Looking to the future, police forces may soon be able to link LFR cameras to trawl large populations, such as Greater London and not just specific localities. There is nothing to regulate this. The public need to be aware of this potential and for there to be an informed scrutiny by Parliament of the risks and benefits.

2. This work follows up on our earlier report *Technology rules? The advent of new technologies in the justice system*, published on 30 March 2022.<sup>1</sup> The Government responded to that report on 23 June 2022<sup>2</sup>, but we wrote to your predecessor saying that we were ‘disheartened’ by the response.<sup>3</sup> Since then, the Government has highlighted the importance of AI, hosting the AI Safety Summit at Bletchley Park in

---

<sup>1</sup> Justice and Home Affairs Committee, *Technology rules? The advent of new technologies in the justice system* (First Report, Session 2021–22, HL Paper 180)

<sup>2</sup> Government response dated 23 June 2022 to JHA Committee’s report *Technology rules? The advent of new technologies in the justice system* (First Report, Session 2021–22, HL Paper 180): <https://committees.parliament.uk/publications/22773/documents/167387/default/>

<sup>3</sup> Letter from Baroness Hamwee, Chair of the Justice and Home Affairs Committee, to Rt. Hon. Priti Patel MP, Home Secretary (6 July 2022): <https://committees.parliament.uk/publications/22973/documents/168396/default/>. The report was debated in November 2022: HL Deb, 28 November 2022, [cols 383GC–414GC](#) (Grand Committee)

November 2023.<sup>4</sup>

3. We have focused on the use of LFR technology rather than other forms of facial recognition technology. On 12 December 2023, the Committee held an evidence session with representatives from the two police forces that currently deploy LFR technology, T/DCC Mark Travis of South Wales Police and Lindsey Chiswick, Director of Intelligence, Metropolitan Police.<sup>5</sup> We also heard from Paul Roberts, Head of Strategy, NEC Software Solutions (the company that provides the software), and Professor Karen Yeung, University of Birmingham. The Committee invited relevant organisations and individuals to submit written evidence.
4. The deployment of LFR during The King’s Coronation in May 2023—described by one academic expert as “probably the largest ever seen in Europe”—brought the technology further into public consciousness.<sup>6</sup> The wider use of LFR technology is being encouraged by the Government. In November 2023, the Minister of State for Crime, Policing and Fire, Rt. Hon. Chris Philp MP, wrote to Chief Constables and Police and Crime Commissioners and said he was “very supportive of the use of Live—or Active—Facial Recognition (LFR) to deter and detect crime in public settings that attract large crowds.”<sup>7</sup>
5. The Committee accepts that LFR may be a valuable tool for police forces, but we are deeply concerned that its use is being expanded without proper scrutiny and accountability. In the letter to Police Chiefs, the Minister claims that there is “a sound legal basis for LFR.”<sup>8</sup> While we acknowledge that the police forces have updated their policies and procedures following the Court of Appeal judgment in *Bridges* in 2020,<sup>9</sup> this turned on a narrow point on equalities, and in any event the Government should not wait for the legality of LFR deployment to be tested again in the courts. We believe that, as well as a clear, and clearly understood, legal foundation, there should be a legislative framework, authorised by Parliament for the regulation of the

---

<sup>4</sup> We note that the Bletchley Declaration acknowledged the risks of AI and welcomed “the recognition that the protection of human rights, transparency and explainability, fairness, accountability, regulation, safety, appropriate human oversight, ethics, bias mitigation, privacy and data protection needs to be addressed.” Prime Minister’s Office, ‘The Bletchley Declaration by Countries Attending the AI Safety Summit, 1-2 November 2023: <https://www.gov.uk/government/publications/ai-safety-summit-2023-the-bletchley-declaration/the-bletchley-declaration-by-countries-attending-the-ai-safety-summit-1-2-november-2023> [accessed 24 January 2024]

<sup>5</sup> Lindsey Chiswick is also the National Police Chiefs’ Council national lead for facial recognition.

<sup>6</sup> ‘Police accused over use of facial recognition at King Charles’s coronation’, *The Guardian* (3 May 2023): <https://www.theguardian.com/uk-news/2023/may/03/metropolitan-police-live-facial-recognition-in-crowds-at-king-charles-coronation>

<sup>7</sup> Home Office and the Rt Hon Chris Philp MP, ‘Letter to Police on AI-enabled facial recognition searches’ (29 October 2023): <https://www.gov.uk/government/news/letter-to-police-on-ai-enabled-facial-recognition-searches> [accessed 18 January 2024]

<sup>8</sup> Home Office and the Rt Hon Chris Philp MP, ‘Letter to Police on AI-enabled facial recognition searches’ (29 October 2023): <https://www.gov.uk/government/news/letter-to-police-on-ai-enabled-facial-recognition-searches> [accessed 18 January 2024]

<sup>9</sup> Written evidence from The Alan Turing Institute ([LFR0001](#))

deployment of LFR technology.

6. We also believe that the Government must lead a wider public debate about the use of LFR technology, as used now and as it develops, to ensure public confidence and support. In response to our original report, the Government said: “Opinion polls consistently demonstrate that police use of technologies such as live facial recognition, which are considered controversial by some, have strong public support.”<sup>10</sup> To us it seems the fact that the technology is regarded as controversial means that continued public support cannot be taken for granted.
7. Our conclusions are outlined in bold and our recommendations or requests for further information are in bold italicised text. We would be grateful for a response to each of them in their sequence, separately, without combining responses to more than one point, before Tuesday 26 March 2024.
8. I am copying this letter to the Rt. Hon. Alex Chalk KC MP, Lord Chancellor; Rt. Hon. Dame Diana Johnson, MP, Chair of the Home Affairs Committee; Rt. Hon. Sir Bob Neill KC (Hons) MP, Chair of the Justice Committee; Joanna Cherry KC MP, Chair of the Joint Committee on Human Rights; and Rt. Hon. Stephen Crabb MP, Chair of the Welsh Affairs Committee. I am also copying it to Mick Antoniw MS, Counsel General for Wales and Hannah Blythyn MS, Deputy Minister for Social Partnership, who have engaged the Committee on some of the issues discussed in this letter.<sup>11</sup>
9. I am coming to the end of my term as Chair of the Justice and Home Affairs Committee, and some of the original members who worked on the *New Technologies* report are also standing down. It will be for my successor to take forward the Committee’s work on this subject, and I am sure the Committee would welcome an early opportunity to speak to you on this and other matters.

Yours Sincerely,



Baroness Hamwee

Chair, House of Lords Justice and Home Affairs Committee

---

<sup>10</sup> Government response to JHA Committee’s report *Technology rules? The advent of new technologies in the justice system* (23 June 2022): <https://committees.parliament.uk/publications/22773/documents/167387/default/>

<sup>11</sup> Justice and Home Affairs Committee, Note of a private meeting held on 16 January 2024 with representatives of the Welsh Government to discuss new technologies and the application of the law (24 January 2024): <https://committees.parliament.uk/publications/43013/documents/214316/default/>

## APPENDIX – JUSTICE AND HOME AFFAIRS COMMITTEE

### Conclusions and recommendations following a short investigation into the use of Live Facial Recognition (LFR) by police forces in England and Wales

In summary, this appendix makes recommendations in relation to:

- The legal foundation for the deployment of LFR technology (paragraph 5)
- The need for clear standards and regulation in relation to the use of LFR (paragraphs 10, 11, 12, 21, 22 and 23)
- The need to future proof these structures and regulation to allow for rapid advancement in the technology (paragraph 27)
- The need for consistent training in the use of LFR across England and Wales (paragraphs 7, 14 and 20)

#### *Legislative basis*

1. Live Facial Recognition (LFR)—the technology that compares a live camera video feed of faces against a predetermined watchlist of people to find a possible match—is used in England and Wales by The Metropolitan Police (Met Police) and South Wales Police. Deployments in London have taken place at least since early 2020<sup>12</sup>, with trials running since 2016.<sup>13</sup> The most recent deployments have been in the Westminster area and Croydon.<sup>14</sup> Instances of extensive crowd scanning have taken place in Oxford Circus and during the Coronation.<sup>15</sup> South Wales Police’s exploration started prior to the UEFA Champions League taking place in South Wales in 2017.<sup>16</sup>
2. Big Brother Watch stated that “There is no legislative basis that creates the police powers for the use of LFR”.<sup>17</sup> The Met Police conceded that there is no specific legislative authority for the deployment of this technology.<sup>18</sup> We were reminded that in 2019, the House of Commons Science and Technology Committee called for a moratorium on the current use of facial recognition technology “until a legislative framework had been introduced and guidance on trial protocols, and an oversight and evaluation system, has been established.”<sup>19</sup>

---

<sup>12</sup> Metropolitan Police (@metpoliceuk), tweet on 24 January 2024]:

<https://twitter.com/metpoliceuk/status/1220663366085115904?lang=en-GB>

<sup>13</sup> Q 3 (Lindsey Chiswick)

<sup>14</sup> Respectively: Westminster Police/Central West BCU (@MPSWestminster), tweet on 10 January 2024:

<https://x.com/MPSWestminster/status/1745063320485331041?s=20> and

Croydon MPS @MPS Croydon, tweet on 19 January 2024,

<https://x.com/MPSCroydon/status/1748314428531970325?s=20>

<sup>15</sup> Respectively: Metropolitan Police Service, *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 17 January 2024] and London Assembly, ‘Facial Recognition Technology’ [www.london.gov.uk/who-we-are/what-london-assembly-does/questions-mayor/find-an-answer/facial-recognition-technology-coronation](http://www.london.gov.uk/who-we-are/what-london-assembly-does/questions-mayor/find-an-answer/facial-recognition-technology-coronation) [accessed 17 January 2024]

<sup>16</sup> Q 3 and Q 5 (T/DCC Mark Travis)

<sup>17</sup> Written evidence from Big Brother Watch ([LFR0002](#))

<sup>18</sup> Q 2 (Lindsey Chiswick)

<sup>19</sup> Science and Technology Committee, *The work of the Biometrics Commissioner and the Forensic Science Regulator* (Nineteenth report, Session 2017–19, HC 1970), paragraph 37.

3. A key legal test for the use of the technology was the case of Mr Edward Bridges, a civil liberties campaigner, who brought a claim against South Wales Police for using live facial recognition technology on a number of grounds, including non-compliance with the public sector equality duty.<sup>20</sup>
4. Lindsey Chiswick of the Met Police argued that the Bridges judgment “found that common law was sufficient” as a basis for the deployment of LFR. The South Wales Police stated that the Bridges case “was really helpful for policing in the absence of ... clarity.” The Met Police’s “legal mandate” document, based upon common law, is also in their view “underpinned” by the College of Policing’s Authorised Professional Practice.<sup>21</sup> They also felt that they were overseen by certain bodies and commissioners who ensure that they act in accordance with their legal mandate and the APP guidance. The South Wales Police noted that they follow the judgment of the Bridges Case and are scrutinised by their internal ethics committees and their commissioner.<sup>22</sup> **We note that, in contrast to the evidence we have received from the police, the Court of Appeal in the Bridges judgment expressed concerns about the “fundamental deficiencies” in the current legal framework arguing that “too much discretion is currently left to individual police officers” and that it is not “clear that there are any criteria for determining where AFR can be deployed” (see paragraphs 91 and 92 of the Court’s decision).**<sup>23</sup> **We are concerned that the findings of the Bridges case were specific to that case and that the case cannot be understood as a clear basis for the use of LFR. Whatever the practice, it requires a firm foundation in primary legislation.**
5. The Government also claims that there is “a sound legal basis for LFR.”<sup>24</sup> **We believe that there should be a legislative framework for the deployment of LFR technology. We invite the Government to explain in full how it has reached its own assessment, and whether it agrees with the Met Police’s view that common law is sufficient for LFR deployment.**

#### *A framework for Deployment and Regulation*

6. At the time of writing, “it is only South Wales [Police] and the Met Police that have access to the technology” in the sense that they are the only forces that have the necessary contracts with the provider.<sup>25</sup> However, South Wales Police have authorised the deployment of the equipment out of South Wales to

---

<sup>20</sup> Royal Court of Justice, *R v The Chief Constable of South Wales Police*, [2020] [EWCA Civ 1058](#)

<sup>21</sup> [Q 2](#) (Lindsey Chiswick and T/DCC Travis)

<sup>22</sup> [Q 2](#) (T/DCC Travis)

<sup>23</sup> Royal Court of Justice, *R v The Chief Constable of South Wales Police*, [2020] [EWCA Civ 1058](#). AFR is used here to mean Automated Live Facial Recognition.

<sup>24</sup> Home Office and the Rt Hon Chris Philp MP, ‘Letter to Police on AI-enabled facial recognition searches’ (29 October 2023): <https://www.gov.uk/government/news/letter-to-police-on-ai-enabled-facial-recognition-searches> [accessed 18 January 2024]

<sup>25</sup> [Q 6](#) (Lindsey Chiswick)

Northamptonshire Police when LFR was deployed during the Silverstone Formula 1 weekend, and a mutual aid operation to Essex Police.<sup>26</sup> Temporary Detective Chief Constable of South Wales Police Mark Travis explained that: “the way it works is that we authorise the deployment of the equipment to another force. The force that it goes to then works through its own policy procedure to determine what it has sitting on its watchlist ... The local force makes a determination in relation to the necessity and the proportionality of the use of the equipment”.<sup>27</sup> **We are concerned by the way that the use of the technology is being expanded to other police force areas by this process, which seems to leave discretion to the recipient police forces in how to employ LFR. Please explain in detail how this process operates, including the safeguards that apply, the contractual role of the software provider, and what liability rests with the providing force when the technology is used in these situations.**

7. The Met Police and South Wales Police are trained in the usage of LFR by the provider, NEC Software Solutions (NEC).<sup>28</sup> T/DCC Mark Travis told us that when South Wales Police lend their equipment to another force, “our trained staff go with it to make sure that the application and the use of the equipment is consistent wherever it is deployed.”<sup>29</sup> **To ensure consistency, as LFR technology is rolled out, we recommend the adoption of a national compulsory training programme and standards for England and Wales to which all police forces must adhere.**
8. We were told that the focus of LFR technology’s deployment aims to tackle “the most serious crime and the most serious vulnerability”.<sup>30</sup> T/DCC Mark Travis referred to terrorism and violence against women and girls, as well as “acquisitive crimes”.<sup>31</sup> Lindsey Chiswick of the Met Police specified that local watchlists include “prolific shoplifting offenders who we have seen in the media that the shops are desperate to catch”<sup>32</sup> as well as those who “fit into the really serious crime categories”<sup>33</sup> such as murderers and rapists. We were also told that Met Police engages “with local shops, local businesses, retail or wherever we are going to deploy it. ‘Serious’ for them is probably quite different from serious in another scenario.”<sup>34</sup> **How is “serious crime” defined and is the definition standard for all forces? How does any definition impact the police’s assessments of necessity and proportionality when deploying LFR technology in a particular situation?**

---

<sup>26</sup> Q 5 (T/DCC Mark Travis)

<sup>27</sup> Q 5 (T/DCC Mark Travis)

<sup>28</sup> Q 6 (Paul Roberts, Head of Strategy, NEC Software Solutions)

<sup>29</sup> Q 6 (T/DCC Mark Travis)

<sup>30</sup> Q 1 (T/DCC Mark Travis)

<sup>31</sup> Q 1 (T/DCC Mark Travis)

<sup>32</sup> Q 5 (Lindsey Chiswick)

<sup>33</sup> Q 5 (Lindsey Chiswick)

<sup>34</sup> Q 7 (Lindsey Chiswick)

9. Lindsey Chiswick explained that watchlists are based on “crime types” rather than by seeking specific known individuals. In the case of the Met Police, the watchlist is approved by an “authorising officer”, who must be superintendent level or above.<sup>35</sup> South Wales Police stated that in the case of Northamptonshire police, the deployment of LFR technology related to a “believed intent that people would try to access an environment that would put their lives or the lives of other people at risk”.<sup>36</sup> In announcing a recent deployment in Croydon, the Met Police issued the following notice on social media: “We’ll be using Live Facial Recognition technology at key locations in Croydon today. This technology helps keep Londoners safe and will be used to find people who *threaten* or cause harm, those who are wanted or have outstanding arrest warrants issued by the court” (emphasis added).<sup>37</sup> **We are concerned by the fact that watchlists include people who “have an intent” or are thought to “threaten” to commit a crime. Such evaluation is most sensitive. What precisely does it mean? Should the approval of watchlists be carried out by a third independent party, outside the police force itself?**

10. In respect of the deployment of LFR, Lindsey Chiswick acknowledged that there is a “balance between security and privacy” but was satisfied that the balance is right.<sup>38</sup> Professor Karen Yeung, pointed out that in 2022, 144,000 faces were scanned by the Met Police, activity that in her view was a “prima facie violation” of those people’s privacy. She noted that eight arrests were made, none for serious crimes, despite the claims that only serious crimes are included on the watchlist.<sup>39</sup> **We recommend the publication of national regulation or at the least guidelines, kept under review, on how extensive crowd-scanning activity is being assessed with relation to its lawfulness, necessity, and proportionality, before and after the deployment of LFR.**

11. It emerged that when a police force uses (or borrows) LFR technology, it is their choice how a watchlist is going to be populated. It is appreciated that Ms Chiswick, as National Police Chiefs’ Council national lead for facial recognition, runs a strategic board and bimonthly working groups where they “pool” their advice nationally on the usage of LFR.<sup>40</sup> **Given the importance of choosing who ends up on a watchlist, we recommend that watchlists should be subject to specific compulsory statutory criteria and standardised training.**

---

<sup>35</sup> Q 1 (Lindsey Chiswick)

<sup>36</sup> Qv 5 (T/DCC Mark Travis)

<sup>37</sup> Croydon MPS @MPSCroydon, tweet on 19 January 2024,

<https://x.com/MPSCroydon/status/1748314428531970325?s=20>. See also the notices on 23 January and 25 January, Croydon MPS @MPSCroydon, tweet on 23 January 2024,

<https://x.com/MPSCroydon/status/1749763976513106210?s=20> and Croydon MPS, @MPSCroydon, tweet on 25 January 2024, <https://x.com/MPSCroydon/status/1750487469399646457?s=20>

<sup>38</sup> Q 5 (Lindsey Chiswick)

<sup>39</sup> Q 5 (Professor Karen Yeung, Interdisciplinary Professorial Fellow in Law, Ethics and Informatics at Birmingham Law School & School of Computer Science)

<sup>40</sup> Q 6 (Lindsey Chiswick)

## Public confidence

12. We are concerned that the public cannot trust the use of LFR without clarity of the legal basis for its use, a fundamental matter which should be clear before particular deployments are addressed. The Met Police and South Wales Police use social media and their websites to announce their deployments of LFR, as well as street signage. Both police forces publish figures on their website about their deployments. The Met Police told us that they “need to do better on communications and find different ways of engaging with people”.<sup>41</sup> The campaign group, Big Brother Watch, has observed that signage at deployments, which alerts members of the public that they are in an area where LFR is being used, has become smaller.<sup>42</sup> **Current means of letting the public know that LFR is to be, and is being, deployed are insufficient. Pre-deployment communication must be standardised through a national, clear and enforceable procedure.**
13. The Met Police referred to surveys indicating that “between 60 and 80% of the public support law enforcement using the technology”, but also conceded that in certain specific community groups the support levels drop.<sup>43</sup> The Met Police told us how they meet independent advisory groups, do some work with young people and with different local community groups. Before deployments, they engage with the local community to understand how people feel about the technology.<sup>44</sup> **We agree that local engagement about the deployment of LFR is crucial in maintaining public trust about the technology. Public attitudes towards the use of LFR technology should be regularly assessed.**
14. We were told that *the design* of LFR applications is a focal point to keep “the human in the loop” to “ensure that, where we provide an alert or a notification, we are really drawing someone’s attention to look at something. We are not providing a direct call to action or a direct instruction. No decision has been made.”<sup>45</sup> **Keeping the ‘human in the loop’ means that the ultimate decision about when to act following an alert must be that of a trained officer. To make sure that this applies in practice and that human/technology interaction is truly meaningful, we recommend that the Home Office requires feedback from LFR operators and reports publicly on this.**
15. The Met Police described the role of LFR in the following terms: “All the technology does is up the chances of plucking that face out of a crowd. What comes after that at that point is normal policing and normal officer powers”.<sup>46</sup> According to Met Police’s

---

<sup>41</sup> Q 8 (Lindsey Chiswick)

<sup>42</sup> Written evidence from Big Brother Watch ([LFR0002](#))

<sup>43</sup> Q 5 (Lindsey Chiswick)

<sup>44</sup> Q 8 (Lindsey Chiswick)

<sup>45</sup> Q 7 (Paul Roberts)

<sup>46</sup> Q 5 (Lindsey Chiswick)



data, around 300,000 faces were scanned with LFR in 2023.<sup>47</sup> The ability of scanning large crowds in seconds goes far beyond “normal policing”, or at least traditional police capability. **Policing capabilities are largely amplified through the use of LFR technology. We recommend that information is required to be put in the public domain about the processes that are followed once a member of the public is approached by a police officer, including when they are told that they have been identified following the use of LFR technology.**

16. In our report, *Technology rules? The advent of new technologies in the justice system*, we called for explainability, that is the ability to explain how a specific outcome was reached.<sup>48</sup> When asked how explainability was embedded in LFR technology, Paul Roberts told us that “The face recognition similarity score is kind of accepted as the explainability basis.”<sup>49</sup> He added that the similarity score is what the “computer thinks with confidence is a strong similarity.”<sup>50</sup> **Greater consideration should be given to how explainability can be embedded in the LFR system.**

17. There have been, according to the Met Police and SWP, no formal complaints about the use of the technology so far. Both South Wales Police and the Independent Office for Police Conduct (IOPC) noted that information about making a complaint is available on their vehicles as well as on the police and crime commissioner’s website.<sup>51</sup> Big Brother Watch told us that the lack of complaints depends on “the lack of specific legislation overseeing police use of LFR means there is no legal framework and no prescribed route to redress for individuals who have been misidentified by the technology”.<sup>52</sup>

### *The technology*

18. Both police forces stated that there had been significant improvements in the number of false alerts. South Wales Police told us that, having scanned 819,943 people in the past year, there had been zero errors.<sup>53</sup> The Met Police stated that over 19 deployments, there had been two false alerts.<sup>54</sup> The Alan Turing Institute explained that the outputs of facial recognition technology “are probabilistic and come with confidence levels, meaning there is always margin for error.”<sup>55</sup> Humans interpreting and challenging the results of LFR software is essential in keeping the number of false alerts low. This is a call that operators have to make in a very narrow timeframe.

---

<sup>47</sup> Metropolitan Police Service, *MPS LFR Deployments 2023 – Date*

<https://www.met.police.uk/SysSiteAssets/media/downloads/force-content/met/advice/lfr/deployment-records/lfr-deployment-grid.pdf> [accessed 17 January 2024]

<sup>48</sup> Justice and Home Affairs Committee, *Technology rules? The advent of new technologies in the justice system* (First Report, Session 2021-22, HL Paper 180)

<sup>49</sup> Q 7 (Paul Roberts)

<sup>50</sup> Q 7 (Paul Roberts)

<sup>51</sup> Q 11 (Lindsey Chiswick and T/DCC Mark Travis) and written evidence from the Independent Office for Police Conduct (LFR0003)

<sup>52</sup> Written evidence from Big Brother Watch (LFR0002)

<sup>53</sup> Q 3 (T/DCC Mark Travis)

<sup>54</sup> Q 3 (Lindsey Chiswick)

<sup>55</sup> Written evidence from The Alan Turing Institute (LFR0001)

Paul Roberts, representing the technology company NEC, told us that in facial recognition systems that are not LFR, they “provide lots of tools” to aid in interpreting and challenging the results of the system. However “there is not really the time for that on a live facial recognition deployment ... there is no time window to provide more tooling than the human comparison.”<sup>56</sup> **We are concerned that crucial evaluations in LFR deployment are confined to split-second assessments, increasing the risk of human error.**

19. The essential role of human operators in LFR deployments means that the training provided to these operators must be sufficient. The Alan Turing Institute told us of the risk of “bias reinforcement between human and machine”, which “poorly trained systems” may worsen.<sup>57</sup> Risks such as being overly-reliant on the technology’s ability to identify face matches and bias reinforcement can be addressed by “robust training” for operators, the Alan Turing Institute told us, “reminding them of these risks and ensuring that there are clear strategies in place to help them deal with situations of uncertainty which may arise” from the software’s output.<sup>58</sup> The Met Police told us that every officer involved in LFR deployments will always have a “training input immediately prior to the deployment”, before every deployment, regardless of whether they have already been through training. Their training covers the “human in the loop” and “unconscious bias”.<sup>59</sup>

20. The training available is founded upon training given to police forces by NEC. Paul Roberts told us that they work on a “train the trainer or master trainer model”, where they train people in the police force to then be able to produce their own training for their organisation, as “a customised course locally”.<sup>60</sup> Ms Chiswick told us that in her role for the National Police Chiefs’ Council, they have a strategic board and working groups where they “pool” advice. She stated that they recognised “a bit of a gap” between training offered and that they are working on bringing a national board together to be able to provide advice to other forces interested in using LFR.<sup>61</sup> T/DCC Mark Travis told us that, when equipment is lent to another force, the South Wales Police’s “trained staff” are also present to ensure the use of the software is “consistent”.<sup>62</sup> When the South Wales Police lent their technology to the Northumberland Police, South Wales Police officers were the ones to operate the equipment. **As the human operation of the technology is essential to its success, we believe that there should be a national training programme and standard that all police forces can adhere to in their use of LFR. This would ensure that newcomers would have the advantage of learning from best practice.**

21. There is a public interest in transparency. There are commercial interests in confidentiality as to how products work. Paul Roberts of NEC told us that there is a

---

<sup>56</sup> Q 7 (Paul Roberts)

<sup>57</sup> Written evidence from The Alan Turing Institute ([LFR0001](#))

<sup>58</sup> Written evidence from The Alan Turing Institute ([LFR0001](#))

<sup>59</sup> Q 6 (Lindsey Chiswick)

<sup>60</sup> Q 6 (Paul Roberts)

<sup>61</sup> Q 6 (Lindsey Chiswick)

<sup>62</sup> Q 6 (T/DCC Mark Travis)

“nervousness” around having full transparency into the technology due to the need to keep aspects of the algorithm secret.<sup>63</sup> However, in his view, the aspect which retains secrecy is the input of the model, whilst the output is “very public already”, having been assessed by the NPL and NIST.<sup>64</sup> With regard to the input, he stated that he was willing to look at “a solution” for balancing transparency with the need for secrecy.<sup>65</sup> Professor Yeung noted that the commercial concerns for maintaining an element of secrecy were “legitimate” (due to, for example, the possibility of criminals “gaming” the system) but that this still poses some problems. She noted that in the Bridges case, the underlying training datasets were not exposed in order to fully evaluate the equality implications of the software. She proposed an “independent agency” that scrutinises, evaluates, and tests the technology without making the details public. She told us that “there is a way of mediating those tensions [between secrecy and transparency] through appropriate institutional safeguards and settings, but they are not currently in place.”<sup>66</sup> **We recommend that regulations and standards include the introduction of appropriate institutional safeguards to ensure independent scrutiny of the technology.**

#### *Regulation and oversight*

22. The Algorithmic Transparency Recording Standard (ATRS) was introduced by the Government in November 2021, intended to be a “standardised way of recording and sharing information about how the public sector uses algorithmic tools”.<sup>67</sup> The ATRS arose from a recommendation of the Centre for Data Ethics and Innovation (CDEI) that there should be a “mandatory transparency obligation on public sector organisations using algorithms to support significant decisions affecting individuals”.<sup>68</sup> Despite this, participation in the ATRS is entirely voluntary, and not all algorithms meet the eligibility requirements to be featured in it. **The Committee recommended in 2022 that in order for the ATRS to become a “satisfactory register of algorithms in the public sector”, it should become mandatory, with entries being reviewed by a central body with the power to issue penalties if the ATRS was not completed.**<sup>69</sup> **We reiterate that recommendation.**
23. Two police forces, the Hampshire and Thames Valley Police and the West Midlands Police, have completed algorithmic transparency reports using the Standard as part of

---

<sup>63</sup> [Q 10](#) (Paul Roberts)

<sup>64</sup> [Q 10](#) (Paul Roberts)

<sup>65</sup> [Q 10](#) (Paul Roberts)

<sup>66</sup> [Q 10](#) (Professor Karen Yeung)

<sup>67</sup> Central Digital and Data Office and Centre for Data Ethics and innovation, ‘Algorithmic Transparency Recording Standard’ (Updated 6 December 2021): <https://www.gov.uk/government/publications/algorithmic-transparency-template> [accessed 18 January 2024]

<sup>68</sup> Central Digital and Data Office and Centre for Data Ethics and innovation, ‘UK Government published pioneering standard for algorithmic transparency’ (Published 29 November 2021): <https://www.gov.uk/government/news/uk-government-publishes-pioneering-standard-for-algorithmic-transparency#:~:text=In%20its%20landmark%20review%20into.support%20significant%20decisions%20affecting%20individuals> [accessed 19 January 2024]

<sup>69</sup> Justice and Home Affairs Committee, *Technology rules? The advent of new technologies in the justice system* (First Report, Session 2021-22, HL Paper 180)

its pilot process, which were then published as part of the ATRS collection.<sup>70</sup> However, neither of these police forces have utilised live facial recognition software. The Alan Turing Institute told us that participation in the ATRS could “drive reflective practice” in the “development and deployment of algorithmic technology” and that it would benefit police forces as they would be able to “learn from each other”, improving policy decisions regarding technology and decreasing potential wasted costs.<sup>71</sup> Despite the potential benefits of utilising the ATRS, in our oral evidence session the Met Police and the South Wales Police both stated that they had not completed the Standard, though they both felt that they met the criteria requirements. They committed to making a recommendation that completing the Standard should be included as professional practice for police forces.<sup>72</sup> While both police forces stated their willingness to complete the Standard after the oral evidence session, we remain concerned by the lack of engagement of police forces using LFR with the ATRS as a government initiative prior to our session. **We question whether the ATRS has been sufficiently publicised to public sector bodies, such as police forces, by the Government. We repeat our 2022 recommendation that the completion of the ATRS should become mandatory.**

24. Ethics Panels and committees are used frequently by police forces, though their advice is not binding.<sup>73</sup> These committees are usually general, looking at a range of policing ethics issues, though there are also specialist ethics committees. In the Committee’s previous inquiry into new technologies, we heard that work was being done to “develop a national data ethics governance panel”<sup>74</sup>. The Met Police noted that they follow the “five conditions” set by the London Policing Ethics Panel for the ethical use of LFR, and that they took advice from the Mayor’s Office for Policing and Crime, the Information Commissioner’s Office, and the Biometrics and Surveillance Camera Commissioner. They told the Committee that they were currently talking to the Equality and Human Rights Commission and had ongoing engagement with academics and civil society groups.<sup>75</sup> The South Wales Police have both an internal and external ethics committee supporting them. The South Wales Police expressed that it “would be beneficial if there were a form of central reference that had subject matter expertise” in complex areas such as LFR.<sup>76</sup> The Met Police also expressed that a national data ethics board “would be very useful”.<sup>77</sup> **We question whether local, generalist ethics panels and committees are sufficient as ethical oversight for LFR deployment. A national ethics committee or board with subject expertise could improve this oversight and we recommend consultation with the police**

---

<sup>70</sup> Written evidence from The Alan Turing Institute ([LFR0001](#)) A collection of algorithmic transparency reports completed using the Algorithmic Transparency Recording Standard can be found at Central Digital and Data Office and Centre for Data Ethics and innovation, ‘Algorithmic Transparency ,Recording Standard’ (Updated 6 December 2021): <https://www.gov.uk/government/publications/algorithmic-transparency-template> [accessed 18 January 2024]

<sup>71</sup> Written evidence from The Alan Turing Institute ([LFR0001](#))

<sup>72</sup> [Q 9](#) (Lindsey Chiswick and T/DCC Travis)

<sup>73</sup> [Q 12](#) (Professor Karen Yeung)

<sup>74</sup> Justice and Home Affairs Committee, [Technology rules? The advent of new technologies in the justice system](#) (First Report, Session 2021-22, HL Paper 180) Box 14, page 74

<sup>75</sup> [Q 4](#) (Lindsey Chiswick)

<sup>76</sup> [Q 13](#) (T/DCC Mark Travis)

<sup>77</sup> [Q 13](#) (Lindsey Chiswick)

**as to the establishment of such a committee.**

25. Both the Met Police and the South Wales Police stated their desire for sufficient oversight. Ms Chiswick told us “I want to be overseen by a body with teeth so that I can prove and demonstrate how I am operating.”<sup>78</sup> **We do not consider the current methods of oversight sufficient. We recommend that scrutiny panels, as recommended for Stop and Search, should be employed for LFR also.**
26. The Committee heard from Professor Yeung that the UK is currently an “outlier as a democratic state in the pace at which we are embracing these technologies.”<sup>79</sup> A proposed Regulation of the European Parliament and European Council<sup>80</sup> would mean that police bodies in the EU would require judicial authorisation in order to use real-time biometric data driven by AI. Outside of select law enforcement scenarios, LFR systems will be banned as they are considered to be of “unacceptable risk”.<sup>81</sup> **We question why there is such disparity between the approach of the UK and other democratic states in the regulation of LFR.**
27. Professor Yeung told us that the police would “struggle in making lawful and proportionate decisions” in the deployment of LFR, because “the law is actually very difficult to apply ... I do not think there is enough guidance or that it is clear enough. We need a legislative framework that makes that much more straightforward.”<sup>82</sup> When asked whether the possibility of using multiple cameras to conduct mass surveillance across a city or region is possible, Professor Yeung told us that it is “already possible in so far as the camera infrastructure is already in place, and you just need a very high-quality internet connection to do it ... The capacity to scale up is readily malleable once the infrastructure is in place.” She added that: “You can see the attractions for control within that, and that is why I think that we need to have a specific legislative regime that provides clear and effective safeguards to ensure adherence to respect for democratic rights and freedoms and the rule of law.”<sup>83</sup> **Primary legislation could be kept up to date. We do not believe that regulation, which can more easily be kept up to date, has kept up with technological advances. Current regulation is additionally likely to be inadequate for future technological developments. Technological advances are so rapid that regulation needs to be kept up to date and agile, without constraining users. Several of our recommendations above point to the need for regulation.**

---

<sup>78</sup> [Q 8](#) (Lindsey Chiswick)

<sup>79</sup> [Q 12](#) (Professor Karen Yeung)

<sup>80</sup> On 9 December 2023, the Council and European Parliament reached an agreement on the proposed Regulation laying down harmonised rules on artificial intelligence. 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 <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52021PC0206>

<sup>81</sup> News European Parliament, ‘EU AI Act: first regulation on artificial intelligence’ (Updated 19 December 2023): <https://www.europarl.europa.eu/news/en/headlines/society/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence> [accessed 18 January 2024]

<sup>82</sup> [Q 5](#) (Professor Karen Yeung)

<sup>83</sup> [Q 9](#) (Professor Karen Yeung)

**28. We believe that, as well as a clear, and clearly understood, legal foundation, there should be a legislative framework, authorised by Parliament for the regulation of the deployment of LFR technology and make these recommendations accordingly.**