11 October 2024

Jake Longhorn
Practice Developer
College of Policing
Harperley Hall, Fir Tree, Crook
County Durham
DL15 8DS

Dear Jake Longhorn,

Thank you for reaching out to Privacy International ("PI") concerning the consultation on the data-driven technologies authorised professional practice ("APP"). We welcome the opportunity to engage with the College of Policing on this APP. Due to the nature of our submission, we have opted to respond via letter as opposed to completing the questionnaire; we trust this is in order.

PI is a London-based non-profit, non-governmental organisation (Charity Number: 1147471) that works internationally to protect people's privacy, dignity, and freedoms.[1] Through our work we aim to build a world where technology will empower and enable us, not exploit our data for profit and control. PI works globally with partners, to challenge overreaching state and corporate surveillance so that people everywhere can have greater security and freedom through greater personal privacy.

Through our work, we have researched and analysed data driven technologies and considered their use by law enforcement. We are aware that UK police forces are already deploying certain technologies including live facial recognition technology ("FRT")[2], drones[3], mobile phone extraction[4], social media monitoring[5] and may be using IMSI catchers[6]. These technologies have

[1] Privacy International, "*When Spiders Share Webs": Unveiling privacy threats of EU-Funded INTERPOL policing programme in West Africa* (available here: https://privacyinternational.org/).
[2]Home Office*, Police use of Facial Recognition: Factsheet* (available here: https://homeofficemedia.blog.gov.uk/2023/10/29/police-use-of-facial-recognition-factsheet/).
[3] National Police Chiefs' Council, *Use of Drones in Policing* (available here: https://https://www.npcc.police.uk/our-work/work-of-npcc-committees/operations-coordination-committee/police-use-of-drones/).
[4] Information Commissioner's Office, I*nvestigation report: Mobile phone data extraction by police forces in England and Wales* (available here: https://https://ico.org.uk/about-the-ico/what-we-do/mobile-phone-data-extraction-by-police-forces-in-england-and-wales/).
[5] Privacy International, *How social media monitoring can be used at a protest* (available here: https://privacyinternational.org/explainer/4509/how-social-media-monitoring-can-be-used-protest).
[6] Privacy International, *Remember those IMSI catchers? UK authorities play hide and seek with use of intrusive surveillance technology* (available here: https://privacyinternational.org/news-analysis/5206/remember-those-imsi-catchers-uk-authorities-play-hide-and-seek-use-intrusive).

been reported to be routinely used by police forces in public places and during protests[7]. Some of these technologies deployed enable indiscriminate surveillance of large numbers of people as they go about their daily lives - many of whom are not reasonably suspected of wrongdoing. Therefore, the deployment of these technologies can subject the population to systematic interferences with their rights to privacy, freedom of expression and the right to protest.[8]

Yet despite the grave risk these technologies pose to human rights the police are already choosing to deploy them.[9] For some of these technologies they are doing so within a legislative void. There is no specific legislation pertaining to how some of these technologies are used that ensures appropriate restrictions and safeguards are in place, as we highlighted in the case of FRT.[10] Therefore, we are concerned that this APP enables the police to continue using such technology while essentially bypassing parliamentary scrutiny and debate on certain technologies. The intrusiveness of live FRT and the dangers associated with its potential abuse by the police call for robust safeguards and oversight governing its authorisation and use, should it ever be deemed permissible.[11]

This concern underscores our engagement with, and commentary on the APP. While we recognise that the College of Policing are developing this guide to ensure police procure, deploy and implement data driven technologies in line with existing laws and standards, our view is that current regulatory instruments do not provide sufficient safeguards, oversight and accountability for the deployment of certain data-driven technologies. Considering this, our submission simply notes two high-level concerns: first, we provide more detail on our concerns relating to the legislative void and second, the application of the APP to existing deployments. These concerns are detailed below.

I. Legislative void

[7] Privacy International, *Privacy at public demonstrations* (available here: https://privacyinternational.org/long-read/2164/privacy-public-demonstrations).
[8] United Nations Human Rights Office of the high Commissioner, *The right to privacy in the digital age: report (2021)* (available here: https://www.ohchr.org/en/calls-for-input/2021/right-privacy-digital-age-report-2021 & https://www.ohchr.org/en/documents/tools-and-resources/practical-toolkit-law-enforcement-officials-promote-and-protect-human).
[9] Donna Ferguson, The Guardian, *Police using live facial recognition at British Grand Prix* (available here: https://www.theguardian.com/technology/2023/jul/08/police-live-facial-recognition-british-grand-prix).
[10] Privacy International, *UK MPs Asleep at the Wheel as Facial Recognition Technology Spells the End of Privacy in Public* (available here: https://privacyinternational.org/long-read/5155/uk-mps-asleep-wheel-facial-recognition-technology-spells-end-privacy-public).
[11] Privacy International, Feedback form on the College of Policing's Consultation on Live Facial Recognition Authorised Professional Practice (available here: https://privacyinternational.org/sites/default/files/2021-06/LFRT%20Consultation%20Response%20Final_0.pdf).

We note that the indicated purpose of the APP[12] is to equip police forces with the necessary considerations to make a responsible decision on whether to deploy data-driven technologies. As such, the APP consolidates all the existing legal and regulatory instruments that should already be considered and complied with. Further, we note that the APP is designed to be technologically neutral and would apply to all forms of technology in the same way. However, in our view, some technologies pose so grave a risk to human rights that there is no framework, either technical or legal, that could enable safe deployment in a manner which is consistent and in compliance with the UK's human rights obligations. Existing regulation does not provide sufficient safeguards.

Whilst we acknowledge the APP is designed to assist police forces to come to such a conclusion and through this process, they may choose not to deploy a technology given the threat they pose. However, it will remain a risk that such technologies could be approved for use if the decision-making process is not well-informed, inclusive and evidence based. Furthermore, the police should already be making this assessment when considering deploying technologies in compliance with existing requirements such as the Human Rights Act 1998 (HRA). Yet, they are already deploying data-driven technologies such as live FRT that directly interferes with individual's rights as provided in the HRA.[13] The incompatibility of live FRT with the right to privacy under Article 8 ECHR has already been subject to legal challenge in the UK. In 2020, in the case of Ed Bridges v South Wales Police, the Court of Appeal found that the police's use of FRT breached privacy rights, data protection and equality laws. The Court held that there were "fundamental deficiencies" in the legal framework and that Ed Bridges' rights were breached as a result.[14]

Yet, police forces across the UK are continuing to use live FRT in public spaces.[15] This year there have been several deployments of live FRT by the Metropolitan Police Service (the Met) throughout London for example, in Croydon[16], Tooting[17] and Catford[18]. The police have boasted that these deployments have led to several arrests. However, these related mostly to breaches of bail and tag conditions, and to minor theft, and it is unclear whether they led to any further action. These deployments are taking place in crowded public areas, with limited warning, and without the consent of individuals whose facial data is being processed. It also strongly undermines police

[12] College of Policing, Data-driven Technologies Authorised Professional Practice: Consultation, page 5 (available here: https://assets.college.police.uk/s3fs-public/2024-08/Data-driven-technologies-APP-consultation.pdf).
[13] Note 10 above.
[14] Liberty, *Liberty Wins Groundbreaking Victory Against Facial Recognition* Tech (available at: https://www.libertyhumanrights.org.uk/issue/liberty-wins-ground-breaking-victory-against-facial-recognition-tech/)
[15] Privacy International, *Latest developments with facial recognition technology in the UK* (available here: https://privacyinternational.org/long-read/5322/latest-developments-facial-recognition-technology-uk).
[16] Anna O'Neill & PA Media, BBC , *Croydon: Met Police to continue facial recognition despite concerns* (available here: https://www.bbc.co.uk/news/uk-england-london-68274090).
[17] Jess Warren, BBC Met Police: Live facial recognition cameras result in 17 arrests in south London (available here: https://www.bbc.co.uk/news/uk-england-london-68638348).
[18] Lewisham MPS, x thread (available here: https://x.com/MPSLewisham/status/1769763255843537209).

claims of FRT being a targeted measure for serious crimes.[19] These deployments are interfering with individuals' rights upheld by the HRA. In terms of section 6 of the HRA[20], public authorities, including the police, are not to act in a way that is incompatible with those rights.

The issue is threefold – first, the police should already be assessing the deployment of data driven technologies in accordance with the laws and regulation outlined in the APP, yet based on their current deployments this doesn't appear to be the case. Second, whether the APP will help officers come to a legally compliant decision around deployment is not guaranteed and; third, there is a bigger issue around the need for specific laws pertaining to these technologies to impose restrictions and safeguards for their use. Although we note the last issue is not within the scope of the College of Policing's mandate to introduce such legislation. Nevertheless, we reiterate that if the police seek to use certain technologies, particularly FRT, it must be introduced via primary legislation and subject to Parliamentary scrutiny.[21] And we would encourage the APP to acknowledge the legislative void currently at play when it comes to the deployment of many of these technologies.

II. Application of the APP to existing deployments

The APP is pitched at the adoption phase and is silent on its application to technologies already deployed, if at all.

As noted above, police forces across the UK are already routinely using data-driven technologies. The assumption seems to be that such deployments were authorised with due regard to the existing regulatory framework, yet the police continue to deploy data-driven technologies in a way that interferes with individual's rights. We are concerned that such technologies already in deployment may bypass the continued-monitoring processes envisaged by the APP. This includes a process to halt deployment after the identification of any serious issues. This is a welcome inclusion considering the evolving nature of the risks they pose. However, the APP does not explicitly state that technologies deployed before the introduction of the APP should also be subject to the continuous monitoring processes.

This lacuna poses a risk that any technology deployed before the introduction of the APP can continue to be used without any evaluation into its ongoing use. In our view, this undermines the aim of the APP to "provide the public with clear assurances of the safeguards in place for the

[19] Biometric Update, *The use of live FRT by British police makes the UK an outlier among democratic states (available here:* https://www.biometricupdate.com/202402/the-use-of-live-frt-by-british-police-makes-the-uk-an-outlier-among-democratic-states)
[20] Section 6 of the Human Rights Act 1998 (available here: https://www.legislation.gov.uk/ukpga/1998/42/section/6).
[21] Note 11 above.

responsible use of DDTS by policing".[22] Any responsible use of technology should assess evolving risks. As such, we recommend that you include an explicit provision on how the APP applies to already-deployed technology. We recommend that already adopted technologies should be subject to the requirements of continuous monitoring.

Conclusion

Thank you for the opportunity to comment on the APP. We look forward to future engagements with the College of Policing on this matter and are available to discuss this submission further with you directly.

Yours sincerely,

Privacy International

[22] Page 5 of the College of Policing 'Data-driven Technologies Authorised Professional Practice: Consultation'.