Liberty— Written evidence (NTL0020)

INTRODUCTION

1. Liberty welcomes the opportunity to respond to the call for evidence on new technologies and the application of the law. We confine our comments to Questions 1, 2, 3, 4, 7, and 10.

QUESTION 1
Do you know of technologies being used in the application of the law? Where? By whom? For what purpose?

2. Liberty is aware of potential deployment of Live Automated Facial Recognition Technology (LFR) by police, as well as use of LFR by private companies, often in conjunction with police. Due to the secretive nature in which LFR has been used, Liberty is yet to confirm whether the technology has been in use since the Court of Appeal's judgment in *R (Bridges) v South Wales Police* [2020] EWCA Civ 1058 ('Bridges') which ruled that police use of LFR was unlawful.

3. In addition, we are aware of surveillance technology being used in the application of the law in other contexts. Liberty has previously revealed that police forces across the UK are using predictive policing programmes to predict where and when crime will happen – and even who will commit it.[1] In brief, predictive mapping programs evaluate police data about past crimes and identify "hot spots" or "boxes" of high risk on a map. Police officers are then directed to patrol these areas – often areas in which local communities are subject to over-policing (that is, a level of policing that is disproportionate to the level of crime that actually exist in a given area). In 2018, we sent 90 Freedom of Information Act (FOIA) requests to every police force in the UK to gain insight into these troubling practices. Subsequently, we revealed that 14 police forces had already rolled out predictive policing technologies or were planning to do so, without proper consideration of human rights and the discriminatory impact these technologies can have. We remain concerned that such technologies entrench pre-existing patterns of discrimination by using biased police data; may result in individualised risk-profiling that targets individuals for surveillance; and fundamentally lack transparency, meaning that effective scrutiny is near impossible.

4. More recently, the organisation Bail for Immigration Detainees (BID) revealed in March 2021 that the Home Office had quietly rolled out new GPS technology for the electronic monitoring of people on immigration bail.[2] Liberty and BID organised an open letter from more than 40 migrants' rights and privacy and tech rights' groups highlighting concerns over the intrusive and punitive nature of the policy, as well as the highly concerning implications of the policy for people's data rights.[3]

---

[1] Couchman, H., *Policing by Machine*, Liberty, January 2019, available at: https://www.libertyhumanrights.org.uk/issue/policing-by-machine/
[2] Bail for Immigration Detainees, *BID's Briefing on Electronic Monitoring,* 24 March 2021, available at: https://www.biduk.org/articles/805-bid-s-briefing-on-electronic-monitoring
[3] Mallinson, M., *Home Office condemned for forcing migrants on bail to wear GPS tags*, The Guardian, 14 June 2021, available at: https://www.theguardian.com/global-development/2021/jun/14/home-office-condemned-for-forcing-migrants-on-bail-to-wear-gps-tags

QUESTION 2

What should new technologies used for the application of the law aim to achieve? In what instances is it acceptable for them to be used? Do these technologies work for their intended purposes, and are these purposes sufficiently understood?

5. When considering new technologies used for the application of law, Liberty believes that the primary considerations should not only be the nature of the technology itself, but the underlying policy rationale of the law. Crucially, when it comes to laws and policies engaging human rights, the key questions are whether the laws and policies themselves are adequately prescribed by law, necessary, and a proportionate means of achieving a legitimate aim - which extends to the technology that is being used to implement the specific law and policy. An additional question arises as to whether the use of technology to apply the law will result in unlawful discrimination.

6. The use of GPS tracking for people on immigration bail is a useful example of why it is not possible to abstract a technological solution from the fundamental problem it is trying to solve, and indeed, how looking at the fundamental aim of a given policy can show that the use of certain technologies can be disproportionate and harmful even if it is being used for its intended purposes. Immigration bail is an administrative tool for contact management of people liable to be detained. It should not be used to coerce or punish and bail conditions must be proportionate in order to be lawful. However, multiple facets of the Home Office's shift from using radio frequency tags to GPS tracking for people on immigration bail have led BID and Liberty to conclude that it is punitive, disproportionate, and potentially unlawful.

7. First, electronic monitoring of any kind already amounts to a significant interference with individual liberty and privacy, and the psychological harm caused by electronic monitoring is well-documented – tag-wearers report that tags have an impact on almost every area of life including the ability to participate in society; relationships; financial and emotional stress; sleep; feelings of dehumanisation and stigma.[4] The Supreme Court has accepted that curfews (which are part and parcel of electronic monitoring immigration bail conditions) amount to a form of detention.[5] GPS monitoring is, however, far more intrusive, and closer to imprisonment, than curfews, with a greater psychological impact. It effectively amounts to an extension of immigration detention outside the physical walls of immigration removal centres or prisons. It is unclear what the intended purpose of electronic monitoring is in relation to immigration bail if immigration bail is supposed to be a primarily administrative rather than a policy designed to punish people on bail, including through surveillance. Moreover, absent an evidence base demonstrating why radio frequency tags were ineffective at meeting the intended aim of an electronic monitoring condition, it is unclear why a more intrusive form of monitoring like GPS is necessary and justifiable.

---

[4] Bhatia, M., (2021), *Racial surveillance and the mental health impacts of electronic monitoring on migrants*, Race and Class, available at: https://journals.sagepub.com/doi/abs/10.1177/0306396820963485

[5] The Queen (on the application of Jalloh) v Secretary of State for Home Department [2020] UKSC 4, 12 February 2020, where the Supreme Court found that unlawful curfews of this nature amounted to false imprisonment.

8. Second, it is highly concerning that the Home Office has given itself almost unlimited discretion to retrospectively access people's 24/7 geolocation data. Under the new GPS monitoring policy,[6] people's 24/7 geolocation data will be collected, processed and retained by the private subcontractor – Capita. The Home Office will subsequently be able to access this data under certain circumstances including "where it may be relevant to a claim by the individual under Article 8 ECHR".[7] Article 8 claims relate to a person's family or private life and may involve considerable personal and private details about an individual's life. A fundamentally dangerous implication of this proposal is that people who make human rights claims will now be required to give the state carte blanche to access highly personal and sensitive geolocation data—simply because it "may be relevant" to their claim.

9. This attempt to harvest immense volumes of geolocation data for purposes that go far beyond monitoring compliance with bail conditions was neither foreseen nor debated by Parliament. This is in stark contrast with the use of electronic monitoring in the criminal justice system, where electronic monitoring data must only be "processed for specified, explicit and legitimate purposes". Indeed, we are seeing a similar pattern where the roll-out of different controversial technologies engaging human rights has taken place without effective scrutiny, including but not limited to the use of facial recognition[8] and predictive policing systems.[9]

10. The rollout of GPS monitoring for people on immigration bail is a clear example of the danger of attempting to assess the acceptability or effectiveness of technology without a clear link to the laws and policies that they are supposed to apply. It also shows the susceptibility of technologies to 'mission creep' resulting in effects that far exceed any underlying lawful rationale. Just because technology can be used to do certain things, does not mean that such application does not need to robustly justified and subject to scrutiny.

11. Facial recognition technology provides another instructive example of how, even if technologies are deemed to be useful for law enforcement and the detection and prevention of crime, utility is not sufficient justification in and of itself. Indeed, it is often precisely because certain technologies are particularly intrusive and oppressive, that they are 'useful' for law enforcement. It would of course aid in the detection of crime if, say there was a national database of every individual in the UK's face, and the police were able to access it in the course of undertaking their functions. But the actual creation and operationalisation of such a database – not least the ways it would infringe on individuals' right to privacy and turn the presumption of innocence on its head – would be unimaginable in a democratic society. Indeed, it was held in the case of *S and Marper v UK* that while a national DNA database would be extremely helpful for the police, it is disproportionate and unlawful. Given moreover that

---

[6] Home Office, *Immigration Bail Version 9.0*, 15 January 2021, available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1014714/immigration_bail.pdf

[7] Ibid, pg. 27.

[8] Woollacott, E., *UK Government Accused Of Sneaking Through New Live Facial Recognition Rules*, Forbes, 23 August 2021, available at: https://www.forbes.com/sites/emmawoollacott/2021/08/23/uk-government-accused-of-sneaking-through-new-live-facial-recognition-rules/?sh=7df3e29a706f

[9] Couchman, H., *Policing by Machine*, Liberty, January 2019, available at: https://www.libertyhumanrights.org.uk/issue/policing-by-machine/

like any data collected from society, the data used to drive facial recognition programmes will be reflective of pre-existing patterns of discrimination,[10] there is a strong case for arguing that the use of facial recognition technology can never be lawful and must instead be prohibited altogether.

QUESTION 3

Do new technologies used in the application of the law produce reliable outputs, and consistently so? How far do those who interact with these technologies (such as police officers, members of the judiciary, lawyers, and members of the public) understand how they work and how they should be used?

12. The rapid advances in the field of artificial intelligence and machine learning, and the deployment of new technologies that seek to analyse, identify, profile, and predict by police, have a seismic impact on the way society is policed, and represents a huge shift in the relationship between the individual and the State. The implications come not solely from privacy and data protection perspectives, but from the larger question for a democratic society permitting and seemingly condoning the rollout of such intrusive technology. This begs the question therefore, not of whether these technologies can be used correctly and reliably, but whether these technologies should be used at all. With respect to facial recognition in particular, Liberty does not believe the technology can ever be safely deployed in public spaces.

13. In addition to the insurmountable rights abuses posed by facial recognition technology, research into uses of this tech consistently demonstrate that it does not produce reliable outputs, thereby further supporting arguments that against its use. A range of studies have shown facial recognition technology disproportionately misidentifies women and BAME people[11][12] – meaning that people from these groups are more likely to be wrongly stopped and questioned by police, and to have their images retained as the result of a false match. Similarly, the Court of Appeal in Bridges noted that there is scientific evidence that facial recognition can be biased and create a greater risk of false identifications in the case of women and BAME people. When exercising their rights under Articles 8, 10 and 11, members of these groups are likely to be treated less favourably than others in the same position by virtue of their sex or race. Similarly, research has demonstrated how trans and non-binary people are regularly misidentified by the tech, leading these communities vulnerable to situations of embarrassment, and contributing to stigmatisation.[13] Studies have also highlighted the disproportionate misidentification of disabled people by facial recognition technology, and AI more broadly.[14]

---

[10] Goodman et al, 2016, *European Union regulations on algorithmic decision-making and a "right to explanation"*. AI Magazine 38, Available at https://arxiv.org/abs/1606.08813 [Accessed November 2018]

[11] Buolamwini et al (2018), *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, Proceedings of Machine Learning Research, 2018 Conference on Fairness, Accountability, and Transparency

[12] Klare et al (2012), *Face Recognition Performance: Role of Demographic Information*, IEEE Transactions on Information Forensics and Security, Available at: https://ieeexplore.ieee.org/document/6327355.

[13] Privacy International (2021), *Threats in the usage of facial recognition technologies for authenticating transgender identities.* Available at: https://privacyinternational.org/news-analysis/4474/threats-usage-facial-recognition-technologies-authenticating-transgender

[14] Sheri Byrne-Haber (2019), *Disability and AI Bias. Available at:*

14. When researchers observed six test deployments of facial recognition by the Metropolitan Police Services in 2018, the LFR system generated 42 eligible matches. Of these, 16 were judged to be 'non-credible' (i.e. that officers did not believe the image recorded by the technology matched the image on the watchlist). Out of the 22 remaining stops (four attempted interventions were unsuccessful as individuals were lost in the crowd), 14 were verified as incorrect matches following an identity check. Only 8 were verified as correct matches. This means that across all six observed trials, and from all computer-generated alerts, facial recognition matchers were verifiably correct on 8 occasions only (19%).[15]

15. Facial recognition technology also raises problems with watchlist accuracy and many people placed on watchlists are put there on the basis of outdated information. This amounts to individuals being stopped in relation to an offence that was already dealt with by the criminal justice system. However, some have been wanted in relation to minor offences and have been arrested accordingly, despite the fact that the lesser offence would have failed to be sufficiently serious to warrant them being included in the initial watchlist in the first place. This raises serious concerns about how facial recognition is used in practice. Touted as a tool to deal with serious crime, it has in practice been used for minor offences, an abuse of the necessity calculation that has been used as justification for the use of such an intrusive tool.[16]

16. Recently, and in apparent response to the Court of Appeal's judgment in Bridges that ruled use of facial recognition by South Wales Police unlawful, the College of Policing have published draft guidance on the use of facial recognition and the Government is consulting on revisions to the Surveillance Camera Code of Practice.

17. Despite purporting to rectify the issues identified in the Court of Appeal's Judgment in Bridges, the Authorised Professional Practice ('APP') in fact falls foul of many of the issues that in Bridges led the Court to find the use of LFRT breached privacy rights, data protection laws, and equality laws. Any claim that the APP implements the decision in Bridges thus falls down not only on its own terms, but by deeply entrenching the problems that the Court found made use of LFRT by South Wales police unlawful in the first place. Various bodies and Governmental departments such as the College of Policing and the Home Office's attempts to not only bypass the Bridges judgment, but also repeatedly fail to account for the judgment's findings, urgently call into sharp focus the significant and unmitigable rights risks presented by the use of this technology as well as the reality that neither police, nor oversight bodies, understand how this technology can be used.

---

https://sheribyrnehaber.medium.com/disability-and-ai-bias-cced271bd533

[15] Pg.10, Fussey, P., and Murray, D., *Independent Report on the London Metropolitan Police Service's Trial of Live Facial Recognition Technology*, The Human Rights, Big Data and Technology Project, July 2019, available at: https://48ba3m4eh2bf2sksp43rq8kk-wpengine.netdna-ssl.com/wp-content/uploads/2019/07/London-Met-Police-Trial-of-Facial-Recognition-Tech-Report.pdf

[16] Pg.11, Fussey, P., and Murray, D., *Independent Report on the London Metropolitan Police Service's Trial of Live Facial Recognition Technology*, The Human Rights, Big Data and Technology Project, July 2019, available at: https://48ba3m4eh2bf2sksp43rq8kk-wpengine.netdna-ssl.com/wp-content/uploads/2019/07/London-Met-Police-Trial-of-Facial-Recognition-Tech-Report.pdf

18. As alluded to previously, however, Liberty does not believe these failings can ever be mitigated in the use of facial recognition technology, since the technology would still be unjustifiably rights-invading. Moreover, as a police surveillance tool, Liberty is concerned that deployments of this surveillance technology would mirror and exacerbate existing disproportionate policing practices (such as stop and search and the Gangs Matrix) in being most frequently used to monitor people of colour and those on lower incomes. The racial and socio-economic dimensions of police trial deployments thus far are instructive in this regard. For example, the Met has deployed facial recognition at Notting Hill Carnival for two years running, a festival celebrating Black Caribbean culture in the UK, as well as twice in the London Borough of Newham. Newham is one of the UK's most ethnically diverse places and the white British population stands at 16.7%, the lowest in the UK. As a police tool that not only has discrimination embedded within the tech, but also in its deployment, not to mention the ways in which policing as an institution itself has consistently proven to be racist, Liberty believes that facial recognition should never be used in public spaces.

QUESTION 4

How do technologies impact upon the rule of law and trust in the rule of law and its application? Your answer could refer, for example, to issues of equality. How could any negative impacts be mitigated?

19. Technology is fundamentally a tool for the implementation of laws and policies. What this means is that we must first scrutinise how these laws and policies interact with the rule of law, trust in the rule of law and issues of equality. Where a policy or law actively undermines the rule of law, trust in the rule of law, and issues of equality, any technologies used in the application of such policies or laws can only serve to speed up and entrench those harmful effects.

20. One current area of concern for Liberty and other racial justice, police monitoring, criminal justice, and privacy groups, is the potential use of technology in the application of the serious violence duty in the Police, Crime, Sentencing and Courts Bill (PCSC Bill).[17] Part 2, Chapter 1 of the Bill places a new statutory duty on public bodies such as healthcare authorities, youth services, local authorities and education providers to collaborate with each other to prevent and tackle serious violence. We are highly concerned that the duty itself has damaging implications for human rights. In relation to this Call for Evidence, we are highly concerned that the duty will give rise to the expanding use of surveillance and policing technologies that pose similar risks to people's rights.

21. Although the serious violence duty has been touted as a public health, multi-agency approach to serious violence, it is fundamentally a police-led, enforcement-driven strategy. The various bodies subject to the duty are not equal partners: police are given the power to demand information from other bodies (like education authorities, healthcare providers or social workers) and they must acquiesce, regardless of whether they determine sharing the

[17] https://www.libertyhumanrights.org.uk/wp-content/uploads/2020/04/Joint-Briefing-on-Part-2-and-10-PCSC-Bill- Liberty-StopWatch-Fair-Trials-Big-Brother-Watch-Defend-Digital-Me-Medact-Unjus.pdf

information is in the public interest or breaches any of their other legal duties or professional obligations. Furthermore, Clauses 9, 15, 16, and 17 of the PCSC Bill have been drafted to override the professional and legal safeguards around personal data that exist in order to safeguard people's human rights. The broad drafting of the duty under clause 7 means that any information disclosure - whether that is about individuals' health status, religious beliefs or political opinions and affiliations - could ostensibly be justified under the banner of 'preventing and reducing serious violence'.[18] Altogether, these provisions are likely to give rise to significant and severe breaches of individuals' data rights under the General Data Protection Regulation (GDPR) and Data Protection Act (DPA) 2018 and their right to a private life (protected under Article 8 ECHR).

22. We are highly concerned that these provisions – which as established above risk severely eroding people's data rights – may be used as a basis on which to develop intrusive and oppressive policing technologies. In other words, the creation of greater powers of data collection on individuals may give rise to the development of new forms of surveillance technology that allow for the easier and more efficient collection, processing, and deployment of data. As citizens, we engage with a wide range of public bodies in our day to day lives – whether that is our school, GP practice, mental health provider, or local council. Under the provisions in Part 2, Chapter 1, our interactions with different public bodies will effectively become data points that can be shared and used by other agencies (including the police) to glean information and potentially to make decisions about us – without our knowledge or consent.

23. It is not difficult to imagine the eventual design, development, and implementation of a computer programme that attempts to map these data points and to create profiles of individuals based on their past behaviour, as a way of determining their propensity to be involved in serious violence in the future. Indeed, as Liberty has revealed in the past, there are already many predictive policing programmes in use across the country. For example, Durham Police have used a program called Harm Assessment Risk Tool (HART) since 2016. The program uses machine learning to decide how likely a person is to commit a violent or non-violent offence over the next two years. The program gives the person a risk "score" of low, medium or high, and is designed to over-estimate the risk.[19] The program bases its prediction on 34 pieces of data, 29 of which relate to the person's past criminal history. The other pieces of data include personal characteristics such as age, gender and postcode[20], which act as proxies for race by indirectly indicating a person's ethnicity and fuelling the same biases. Research on algorithms used in the criminal justice system in the United States shows that even where race was removed as a category from the inputted data, the algorithm still learned characteristics, or attributes, in a way that is discriminatory.[21]

---

[18] These are subject to a higher degree of protection under both the Data Protection Act 2018 (DPA) and the ECHR.

[19] Oswald et al, 2018, *Algorithmic Risk Assessment Policing Models: Lessons from the Durham HART Model and 'Experimental' Proportionality*, Information & Communications Technology Law, Volume 27, 2018, pages 228-230, Available at: https://ssrn.com/abstract=3029345 [Accessed November 2018]

[20] Oswald et al, 2018, *Algorithmic Risk Assessment Policing Models: Lessons from the Durham HART Model and 'Experimental' Proportionality*, Information & Communications Technology Law, Volume 27, 2018, Available at: https://ssrn.com/abstract=3029345 [Accessed November 2018]

[21] Question 142, Science and Technology Committee Oral evidence: Algorithms in decision-

24. In April 2018, it was revealed that police data fed into the HART system was supplemented using an Experian[22] dataset called "Mosaic", produced through profiling each of the 50 million adults in the UK.[23] Mosaic profiles and classifies people into spurious groups – for example, a *"crowded kaleidoscope"* is a low-income*, "multi-cultural"* family working *"jobs with high turnover"* and living in *"cramped houses"* and *"overcrowded flats"*.[24] Mosaic even links names to stereotypes: for example, people called Stacey are likely to fall under *"Families with Needs"* who receive "a range of benefits". Terrence and Denise are *"Low Income Workers"* who have *"few qualifications"* and are *"heavy TV viewers"*.[25] Running this data through individual risk assessment programs inevitably encourages a discriminatory and offensive association between factors such as family circumstances, income and propensity to commit crime.

25. In and of itself, such technologies are corrosive of the presumption of innocence that undergirds the British legal system. Furthermore, the ways data is collected to fuel these technologies, and their subsequent operationalisation, will have significant consequences for labelled individuals, their families, and their social circles. The failings of the Gangs Matrix are instructive in this regard. It is well-established that the policing of serious violence is heavily fuelled by racial stereotypes, many of which centre on the ill-defined and porous concept of the 'gang'.[26] The stark statistics on the Metropolitan Police Service's (MPS) Gangs Matrix, revealed in a report published in 2018 by Amnesty International, lay bare the over-identification of people of colour as gang affiliated – at the time of publication 72 per cent of individuals on the MPS's Gangs Matrix were black, yet the MPS's own figures show that just 27 per cent of those responsible for serious youth violence are black.[27][28] The persistence of stereotypical assumptions as regards to people who may be involved in serious violence practically ensures that data collected, processed, and deployed in pursuit of this duty through new technologies will be imbued with prejudice, contrary to the right to non-discrimination and the public sector equality duty.[29] The consequences of having been discriminatorily profiled – such as being locked out

---

making, HC 351, 14 November 2017

[22] Experian is a consumer reporting agency. Consumer reporting agencies are companies that collect and sell personal information on consumers that is used to decide whether to provide consumers credit, insurance, medical care, housing, banking services, utilities, and employment.

[23] Big Brother Watch, 2018, *Police use Experian Marketing Data for AI Custody Decisions* [Press release], 6 April, Available at: https://bigbrotherwatch.org.uk/all-media/police-use-experian-marketing-data-for-ai-custody-decisions

[24] Ibid.

[25] Ibid.

[26] Patrick Williams, *Being Matrixed: The (over)policing of gang suspects in London*, August 2018, https://www.stop-watch.org/uploads/documents/Being_Matrixed.pdf

[27] Amnesty International, *Trapped in the Matrix: Secrecy, stigma and bias in the Met's Gangs Database*. May 2018, https://www.amnesty.org.uk/files/reports/Trapped%20in%20the%20Matrix%20Amnesty%20report.pdf.

[28] The West Midlands Police Ethics Committee has raised concerns that active proposals using crime data to identify young 'violent offenders' in school catchment areas would create "risks of stigmatising and labelling children, areas, schools or neighbourhoods)." (published February 2021)) https://www.westmidlands-pcc.gov.uk/archive/ethics-committee-february-2020/ See also: Documents ref 14122020 - EC - Agenda Item 3c - Analysis of school catchment areas and violence – proposal and 14122020 - EC - Minutes Advice For background see article https://www.birminghammail.co.uk/news/midlands-news/fears-over-police-plan-identify-20193614

[29] Section 149, Equality Act 2010.

of public services, housing, and education – are long-lasting, and have the potential to foment alienation and exclusion. [30]

26. The above example - both the law itself, and the potential ways that different technologies might be used to implement it - underscores the importance of applying a rights-based approach to maintain trust and confidence in the rule of law. The way to ensure that technology used in the application of the law does not erode trust in the rule of law, is to ensure that both the law underlying and the use of the technology itself complies with human rights standards and are accompanied by strong and robust safeguards. If such technologies cannot comply with such human rights standards, they must be roundly rejected.

QUESTION 7

How far does the existing legal framework around new technologies used in the application of the law support their ethical and effective use, now and in the future? What (if any) new legislation is required? How appropriate are current legal frameworks?

27. Police use of facial recognition in public spaces is an enormous infringement of privacy for everyone who passes by the camera – and deployments of this surveillance technology are also likely to mirror existing disproportionate policing practices (i.e. stop and search,[31] the Gangs Matrix[32]) in being most frequently used to monitor people of colour and those on lower incomes. Being able to choose when and how to disclose one's identity, and to whom, is at the heart of a person's dignity and autonomy. In some cases, identification determines how the State interacts with people and whether they are afforded access to their rights. The use of facial recognition therefore represents a huge shift in the relationship between the individual and the State, and for our right to remain anonymous more broadly. The human rights impact of its indiscriminate and non-consensual nature means that it should have no place on our streets.

28. In addition to the privacy and discrimination concerns already outlined, facial recognition also poses a significant interference with our freedom of expression and association. For instance, the use of facial recognition technology can be highly intimidating. If we know our faces are being scanned by police and that we are being monitored when using public spaces, we are more likely to change our behaviour.[33] Those changes in behaviour may relate to where we go and

---

[30] Patrick Williams, *Being Matrixed: The (over)policing of gang suspects in London*, August 2018, https://www.stop-watch.org/uploads/documents/Being_Matrixed.pdf

[31] Official figures show people who identify as black in England and Wales are nearly 10 times more likely to be stopped than people who identify as white. See: GOV.UK Ethnicity Facts and Figures, *Stop and Search,* 19 March 2020, Available at: https://www.ethnicity-facts-figures.service.gov.uk/crime-justice-and-the-law/policing/stop-and-search/latest

[32] The Gangs Matrix was part of a highly- politicised response to the 2011 London riots. More than three- quarters (78 per cent) of the 'gang nominals' included on the database are black, a disproportionate number given the Met's own figures show that only 27 per cent of those responsible for serious youth violence are black. See: Wiilliams (2018), *Being Matrixed: The (over)policing of gang suspects in London,* StopWatch, Available at: https://www.stop-watch.org/uploads/documents/Being_Matrixed.pdf

[33] Studies have shown that people were less inclined to attend mosques they thought were under government surveillance. Business owners muted political discussion by turning off Al-Jazeera in their stores, and activists self-censored their comments on Facebook. See: Shamas et al (2103), *Mapping Muslims: NYPD Spying and its Impact on American Muslims*, Muslim American Civil Liberties Coalition (MACLC), and Creating Law Enforcement Accountability & Responsibility

who we choose to associate with. For a whole host of reasons linked to a desire to retain our anonymity and to keep our activities and political views private, we may decide not to attend public meetings, to avoid our local high street, or change who we spend time with in public spaces. For example, Liberty has worked with protesters who expressed how intimidating they found the presence of facial recognition at demonstrations, and who said that they would be reluctant to attend a future protest where it was in use. Forty per cent of people aged 16-24 said they simply would not attend an event where facial recognition was being deployed.[34]

29. Even where images or biometric data are not retained following a deployment of facial recognition, this technology could still be used to identify that a known person was at an event and this could be recorded through traditional methods. The UK has a shameful history of subjecting political activists to invasive state surveillance.[35] The European Court of Human Rights recently held that the UK had violated the right to privacy of Mr John Catt, a peace movement activist who – despite having never being convicted of any offence – had his name and other personal data included in a police database and was subject to intrusive surveillance.[36]

30. If facial recognition interacts with other surveillance technologies, people are increasingly likely to feel that they have no choice but to avoid expressing religious or dissenting political views in public, and may consequently avoid attending demonstrations, political meetings or places of worship. As a society, this will undermine our ability to express ideas and opinions, communicate with others and engage in democratic processes, as people increasingly choose not to pay the price of handing over their sensitive biometric data in order to do so. Therefore, Liberty does not believe that facial recognition technology can ever be used legally, now or in the future.

31. Police deployment of facial recognition was considered by the Court of Appeal in the case of *R (Bridges) v South Wales Police* [2020] EWCA Civ 1058 ('Bridges'). The Court found that South Wales Police's (SWP) use of the technology was unlawful as it was not 'in accordance with law' for the purposes of Article 8(2) of the European Convention on Human Rights (ECHR); that SWP had failed to carry out a proper data protection impact assessment (DPIA); and that they had failed to comply with the public sector equality duty in section 149(1) Equality Act 2010. In other words, the Court of Appeal ruled that there was no adequate legal framework for the lawful use of live automated facial recognition technology.

32. The Government has previously sought to rely on the original High Court judgment in the Bridges case as a legal basis for the roll out of facial recognition technology, stating that "[t]he High Court found that there is a clear and sufficient legal framework for police use of live facial recognition (LFR) in

---

(CLEAR) Project, available at: http://www.law.cuny.edu/academics/clinics/immigration/clear/Mapping-Muslims.pdf

[34] London Policing Ethics Panel, *Final Report on Live Facial Recognition*, 2019, available here: http://www.policingethicspanel.london/uploads/4/4/0/7/44076193/lfr_final_report_-_may_2019.pdf

[35] Lewis, P. and Evans, R., *Secrets and lies: untangling the UK 'spy cops' scandal,* The Guardian, 28 October 2020, available at: https://www.theguardian.com/uk-news/2020/oct/28/secrets-and-lies-untangling-the-uk-spy-cops-scandal

[36] *Catt v United Kingdom* 43514/15, [2019] ECHR 76

England & Wales".[37] Given that this judgment has since been overturned, and the practices of SWP declared unlawful on this specific basis, the Government's position is not tenable and Parliament must once again question the legal framework for its use and lead the debate around whether any legal framework can possibly meet the rights challenges presented by this technology. Liberty's view is that even if there were laws regulating the use of this technology, it would still pose an unacceptable threat to human rights.

33. It is clear from the current and potential future human rights impact of facial recognition that this technology has no place on our streets. There has been no proper parliamentary or public debate about the use of this mass surveillance technology, denying Parliament the opportunity to consider the threat that it poses. The breadth of public concern around this issue is clear. At the time of writing, Liberty's petition calling for a ban against the use of facial recognition in publicly accessible places has over 65,000 signatories,[38] 31 national and international civil society organisations published an open letter calling for facial recognition technology by police and private companies to be banned, [39] and a statement released in September 2019 by Big Brother Watch was signed by politicians from across the political spectrum and 25 race equality and technology campaign groups – as well as technology academics and legal experts.[40] Several cities in the US have banned the use of facial recognition.[41] It is vital that Members of Parliament and Peers demand the opportunity to steer the debate on this significant step change in policing. Whether and how live facial recognition is used by our police forces – a move which fundamentally alters the relationship and balance of power between citizens and the State – should be a matter for Parliament. Should Parliament be afforded this opportunity, it will be evident that legislation attempting to regulate the use of this technology is insufficient – instead, its use in public spaces should be wholly prohibited.

QUESTION 10

This Committee aims to establish some guiding principles for the use of technologies in the application of the law. What principles would you recommend?

34. The use of technologies in the application of the law must be evaluated using a rights-based approach. Just as laws and policies engaging human rights must be adequately prescribed by law, necessary, and a proportionate way of

---

[37] HC Deb 20 Jan 2020 c 5358W

[38] See: https://liberty.e-activist.com/page/46698/petition/1

[39] *Civil Society Groups: Live Facial Recognition Technology should not be used in public spaces*, Privacy International, August 2021, available at: https://privacyinternational.org/sites/default/files/2021-08/LFRT%20Open%20Letter%20Final.pdf

[40] Big Brother Watch, *Joint statement on police and private company use of facial recognition surveillance in the UK*, 2019, available at: https://bigbrotherwatch.org.uk/wp-content/uploads/2019/09/Statement-to-stop-live-facial-recognition-surveillance-BBW-September-2019-1.pdf

[41] Conger, K., Fausset, R., and Kovaleski, S.F., *San Francisco Bans Facial Recognition Technology,* The New York Times, 14 May 2019, available at: https://www.nytimes.com/2019/05/14/us/facial-recognition-ban-san-francisco.html; Ravani, S., *Oakland bans use of facial recognition technology, citing bias concerns*, San Francisco Chronicle, 16 July 2019, available at: https://www.sfchronicle.com/bayarea/article/Oakland-bans-use-of-facial-recognition-14101253.php; Jarmanning, A., *Boston Bans Use Of Facial Recognition Technology. It's The 2nd-Largest City To Do So*, WBUR, 24 June 2020, available at: https://www.wbur.org/news/2020/06/23/boston-facial-recognition-ban

achieving a legitimate aim, the design and implementation of technologies must be subject to similarly robust scrutiny. Additionally, the use of technology in the application of law must also be robustly evaluated in relation to data protection principles and any such application must be adequately communicated to all stakeholders, including those who may encounter particular difficulties accessing this technology, such as people who are digitally excluded and people with protected characteristics.

September 2021