Privacy International's submission in advance of the consideration of the eight periodic report of the United Kingdom, Human Rights Committee, 140th session, March 2024

February 2024

Introduction

The following submission is based on PI's research and analysis of the UK's legislation, policies and practices and draws from the organisation's litigation in UK courts and the European Court of Human Rights on related issues.

This submission covers: the current UK communications' surveillance regime and the proposal for its reform (Article 17 ICCPR); the surveillance of migrants (Articles 7, 17, 24 ICCPR); and the surveillance of peaceful assemblies (Articles 17 and 21 ICCPR.)

1. UK communications' surveillance regime (Article 17)

Contrary to the UK government's assertion, the Investigatory Powers Act 2016 (IPA 2016) does not ensure that interception and access to communications and communications data is carried out in accordance with applicable international human rights standards to respect and protect the right to privacy.

PI maintains that some of the surveillance powers in the IPA 2016 (most notably the bulk powers in Parts 6 and 7) constitute a disproportionate and unlawful interference with the fundamental right to privacy as protected by Article 17 of the ICCPR and Article 8 of the European Convention on Human Rights (ECHR).[1] In the words of the UN High Commissioner for Human Rights, the IPA

[1] See PI's comments during the adoption of the IPA: Privacy International Submission in Response to Science & Technology Committee Call for Evidence on the Draft Investigatory Powers Bill (27 November 2015), https://privacyinternational.org/sites/default/files/2017-12/PrivacyInternational_ScienceTechSubmission.pdf ; Privacy International & Open Rights Group, Submission to the Joint Committee on Human Rights on the Draft Investigatory Powers Bill (7 December 2015), http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/human-rights-committee/legislative-scrutiny-draft-investigatory-powers-bill/written/25654.pdf ; Joint Committee on the Draft Investigatory Powers Bill, Internet service providers and civil liberties groups give evidence (9 December 2015), https://www.parliament.uk/external/committees/joint-select/draft-investigatory-powers-bill/news/2015/civil-liberties-internet-providers-evidence ; PI, Submission to the Joint Committee on the Draft Investigatory Powers Bill (21 December 2015), https://privacyinternational.org/sites/default/files/2017-12/Submission_IPB_Joint_Committee.pdf

2016 constitutes "one of the most sweeping mass surveillance regimes in the world, permitting the interception, access, retention and hacking of communications without a requirement of reasonable suspicion."[2]

Since its adoption in 2016, legal challenges have forced the government to change some parts of the IPA. In particular, as noted in the UK's report, amendments to the communications data regime under the IPA 2016 were made in response to the Court of Justice of the European Union rulings on data retention and acquisition.[3]

Judgments in separate litigation of surveillance practices, including cases brought by Privacy International, also resulted in findings of violations of human rights law related to the application of the IPA.

On 30 January 2023, the Investigatory Powers Tribunal (IPT) held that the intelligence agency MI5 (Security Service) acted unlawfully by knowingly holding and handling people's personal data in systems that were in breach of legal requirements.[4] Specifically, the Tribunal held that "from late 2014, there were serious failings in compliance with review, retention and deletion policies which required urgent action to be taken by the Management Board of MI5" (§§66, 79, and 160). Despite knowing about issues with non-compliance, at the most senior level, MI5 made a positive decision not to report its non-compliance to oversight bodies (§§82, 135, and 147). The IPT also held that the warrants, authorisations, and directions which had been issued by the Secretary of State for the Home Department (Home Office) permitting MI5 to obtain personal data and process it in the non-compliant "technical environments" between late 2014 and April 2019 were unlawful. The warrants did not meet the safeguarding requirements imposed by the applicable legislation (that is the Regulation of Investigatory Powers Act 2000 (RIPA) and the IPA 2016).[5]

Despite these judgments of non-compliance with international and domestic human rights law, the government is currently proposing changes in the IPA regimes that, if adopted, would further undermine the right to privacy instead of addressing the above shortcomings.[6]

---

[2] The UN High Commissioner for Human Rights delivered the following speech at the Law Society in London, 26 June 2017, https://www.unog.ch/unog/website/news_media.nsf/(httpNewsByYear_en)/6B25EB688245C4D0C125814C002FEE4A?OpenDocument

[3] See https://privacyinternational.org/legal-action/cjeu-bulk-challenge

[4] Judgment: https://privacyinternational.org/sites/default/files/2023-01/IPT-20-01-CH%20Judgment%2030%20January%202023.pdf

[5] For details of the case and PI's analysis, see https://privacyinternational.org/legal-action/mi5-ungoverned-spaces-challenge

[6] See the Investigatory Powers (Amendment) Bill (IPAB): https://bills.parliament.uk/bills/3508/publications; see also a joint briefing criticising the IPAB: https://www.openrightsgroup.org/publications/joint-briefing-on-the-investigatory-powers-amendment-bill/

1.2 Expansion of bulk personal datasets and weakening of safeguards

The existing definition of Bulk Personal Datasets (BPDs) under Section 199 of the IPA 2016 is extremely broad, covering any "(a) set of information that includes personal data relating to a number of individuals [and] (b) the nature of the set is such that the majority of the individuals are not, and are unlikely to become, of interest to the intelligence services in the exercise of its functions." In the course of litigation brought by PI against a number of intelligence agencies and the Secretary of State for the Home Department, an MI5 witness acknowledged that the agency held the following categories of BPDs relating to: law enforcement agencies and intelligence, travel (including passports and biometric information contained therein and travel activity), communications, finance, population, and commercial (which provide details of individuals involved in commercial activities).[7]

PI maintains that the current power to obtain BPDs under part 7 of the IPA 2016 constitutes a disproportionate and unlawful interference with the fundamental right to privacy. The acquisition, retention, and use of large databases of information plainly amounts to a serious interference with the right to privacy. In order for such interference to be lawful under domestic and human rights law, powers contained in part 7 must comply with the principles of legality, necessity, and proportionality. We have consistently argued that the power to obtain and retain BPDs, as provided for under part 7 does not comply with these principles.[8]

Regretfully, in the Investigatory Powers Amendment Bill (IPAB), the government seeks to further weaken, amend or remove some of the already minimal safeguards which apply to its BPDs powers. The IPAB introduces "low or no reasonable expectation of privacy" BPDs, which are vaguely defined and subject to lower thresholds for access, including an insufficient form of authorisation. The Bill also proposes permitting the UK intelligence services to access BPDs held by third parties which would reduce the safeguards applied to the collection and retention of such data. Any diminution of safeguards around the acquisition and handling of BPDs would cause irreparable harm to millions of people's fundamental right to privacy and would create unchecked opportunities for state agents to abuse their powers.[9]

---

[7] *Privacy International v Secretary of State for Foreign and Commonwealth Affairs, Secretary of State for the Home Department, Government Communication Headquarters, Security Service, Secret Intelligence Service* [2016] UKIPTrib 15_110-CH.

[8] See, for example our case, *Privacy International v Secretary of State for Foreign and Commonwealth Affairs and others*, IPT/15/110/CH, in which PI challenged the powers governing the acquisition of BPD prior the IPA coming into effect.

[9] For details of PI's position, see https://privacyinternational.org/sites/default/files/2023-07/20230313_PrivacyInternational_ResponsetoIRIPA.pdf ; see also a joint briefing by PI and others criticising the IPAB: https://www.openrightsgroup.org/publications/joint-briefing-on-the-investigatory-powers-amendment-bill/

1.3 Technical capabilities notices and the weakening of encryption

Under the IPA 2016, both National Security Notices (NSN) and Technical Capability Notices (TCN) served by the Secretary of State to telecommunications operators may require them to carry out activities that would facilitate intrusive forms of surveillance such as interception and equipment interference (government hacking.) For example, Section 252(3) IPA 2016 stipulates that an NSN may require an operator to facilitate "anything done by an intelligence service under any enactment other than" the IPA 2016 or "to provide services or facilities for the purpose of assisting an intelligence service to carry out its functions more securely or more effectively", while Section 253(5) IPA 2016 states that a TCN may, among others, include obligations relating to equipment owned by an operator, obligations "relating to the removal by a relevant operator of electronic protection applied by or on behalf of that operator to any communications or data" or obligations relating to the security of the services provided by an operator.

The privacy and security implications of NSNs and TCNs are potentially profound because these notices can require systemic change, demanding that operators alter their services in a way that may affect all users. For instance, a TCN requiring the "removal by a relevant operator of electronic protection" could be used to force a service such as WhatsApp or Apple to remove or undermine the end-to-end encryption of the services it provides worldwide. End-to-end encryption is fundamental for preserving the privacy and security of messages,[10] as noted, inter alia, by resolutions of the UN General Assembly and the UN Human Rights Council.[11]

While the IPA 2016 provides some safeguards, by, for instance, requiring that a "decision to give the notice has been approved by a Judicial Commissioner", its provisions still raise concerns about their compatibility with international human rights law standards. The European Court of Human Rights has applied a heightened standard of 'strict necessity' to interferences with the right to privacy when using "cutting-edge" technologies in a secret surveillance context.[12] Similarly, the UN High Commissioner for Human Rights has highlighted the privacy risks posed by measures that undermine encryption of communications and security of devices through government hacking and he recommended that governments "avoid all direct, or indirect, general and indiscriminate restrictions on the use of encryption, such as prohibitions, criminalization, the imposition of weak encryption standards or requirements for mandatory general client-side scanning; interference with the encryption of private communications of individuals should only be carried out when authorized by an independent judiciary body and on a case-by-case basis, targeting individuals if

[10] See, See PI, Securing Privacy: PI on End-to-End Encryption, https://privacyinternational.org/report/4949/securing-privacy-end-end-encryption
[11] See A/RES/77/211 and A/HRC/RES/48/4.
[12] *Szabó and Vissy v Hungary*, App No 37138/14, ECtHR, § 73 (12 January 2016); see also, *Liblik and Others v Estonia*, App Nos 173/15 and 5 others, ECtHR, § 131 (28 May 2019) ("powers to instruct secret surveillance of citizens are only tolerated under Article 8 to the extent that they are strictly necessary for safeguarding democratic institutions".)

strictly necessary for the investigation of serious crimes or the prevention of serious crimes or serious threats to public safety or national security".[13]

The proposed changes contemplated by the government would, inter alia, seek to impose a requirement for operators to notify the Secretary of State of any proposed "relevant changes" to their technical systems, which include changes in the capabilities of an operator to provide the intelligence services with communications data and/or content.[14] It appears to be squarely aimed at innovations and updates to encryption technology and crucial security patches, whose main purpose is to keep devices and data infrastructure secure. By requiring such notification, the government may both (i) slow down the implementation of important privacy and security improvements, as notice must be provided a "reasonable period" before implementation, and (ii) could use its TCN and NSN powers to prevent changes to which it objects.[15] The exercise of this notification requirement also lacks prior independent authorisation, which runs counter the Human Rights Committee's Concluding Observations on the Seventh Periodic Report of the United Kingdom of Great Britain and Northern Ireland, which recommended that "The State Party should: […] (c) Ensure that robust oversight systems over surveillance, interception and intelligence-sharing of personal communications activities are in place, including by providing for judicial involvement in the authorization of such measures in all cases".[16]

The government is further seeking to expand the extraterritorial application of TCNs, NSNs and the new notification requirement.[17] While the IPA 2016 already claims extraterritorial application,[18] the IPAB suggests that the obligations contained in a notice served by the Secretary of State upon the UK establishment of an operator would apply to the activities of that operator everywhere else despite its corporate structure or other relevant legal regimes.

As a result, if the UK Government decides to undermine end-to-end encryption, by using the proposed changes to the notices regimes, then end-to-end encryption will also be weakened for citizens in states with authoritarian regimes and a weak rule of law, where communications channels that offer advanced security are often the sole means for lawyers, researchers, civil society, activists, human rights defenders, marginalised and vulnerable groups (including based on gender, religion, ethnicity, national origin or sexuality) and artists to avoid persecution.[19] As

[13] Report of the UN High Commissioner for Human Rights on the right to privacy in the digital age, 4 August 2022, UN Doc A/HRC/51/17, para 57(b).
[14] See the Investigatory Powers (Amendment) Bill (IPAB), Clause 20, https://bills.parliament.uk/bills/3508/publications
[15] See a joint briefing by PI and others criticising the IPAB: https://www.openrightsgroup.org/publications/joint-briefing-on-the-investigatory-powers-amendment-bill/
[16] 17 August 2015, UN Doc CCPR/C/GBR/CO/7, para 24.
[17] See the Investigatory Powers (Amendment) Bill (IPAB), https://bills.parliament.uk/bills/3508/publications
[18] See for example Section 253(8) IPA 2016: "A technical capability notice may be given to persons outside the United Kingdom (and may require things to be done, or not to be done, outside the United Kingdom)")
[19] See, UN General Assembly Resolution on the Safety of Journalists and the Issue of Impunity, UN Doc A/RES/74/157 (18 December 2019): "Emphasizes that, in the digital age, encryption and anonymity tools have become vital for many journalists to freely exercise their work and their enjoyment of human rights, in particular their rights to freedom of expression and to privacy, including to secure their communications and to protect the confidentiality of their sources, and calls upon States not to interfere with the use of such

the UN High Commissioner for Human Rights has underlined, "where a State exercises regulatory jurisdiction over a third party that controls a person's information (for example, a cloud service provider), that State also has to extend human rights protections to those whose privacy would be affected by accessing or using that information".[20] In particular, in relation to access to encrypted communications, the UN High Commissioner for Human Rights noted that "encryption and anonymity tools are widely used around the world, including by human rights defenders, civil society, journalists, whistle-blowers and political dissidents facing persecution and harassment. Weakening them jeopardizes the privacy of all users and exposes them to unlawful interferences not only by States, but also by non-State actors, including criminal networks".[21]

2. Electronic surveillance of migrants through GPS ankle tags (Articles 7, 17 and 24)

As part of a broad range of surveillance measures targeting migrants,[22] the UK's Home Office has rolled out the imposition of GPS ankle tags on migrants, a highly punitive surveillance measure. The stated objective of the measure according to the government is to prevent migrants from absconding and to monitor their compliance with immigration bail conditions, but the Home Office has granted itself in policy the right to use GPS tags' location data for other non-statutory purposes.[23]

Currently, it is mandatory for Foreign National Offenders to be subject to electronic monitoring when released on immigration bail.[24] However, anyone subject to immigration control, including asylum seekers in the course of their application or other proceedings, can be subject to GPS tagging. An "Expansion Pilot" was also commenced in June 2022 and extended in June 2023, testing the application of GPS tagging to all asylum seekers who arrive to the UK by "unnecessary and dangerous routes".[25] There is no time limit for how long an individual must wear a tag, hence some people are tagged for years while they await decisions on their immigration applications, or await deportation.

technologies and to ensure that any restrictions thereon comply with States' obligations under international human rights law."

[20] Report of the United Nations High Commissioner for Human Rights on the Right to Privacy in the Digital Age, UN Doc A/HRC/39/29 (3 August 2018), para 36.

[21] Ibid, para 20.

[22] For an overview, see Privacy International, Protecting migrants at borders and beyond, https://privacyinternational.org/protecting-migrants-borders-and-beyond; and 10 threats to migrants and refugees, https://privacyinternational.org/long-read/4000/10-threats-migrants-and-refugees

[23] Home Office, Immigration Bail Version 18.0, 30 November 2023, https://assets.publishing.service.gov.uk/media/6568977d2ee693000d60cb75/Immigration+bail.pdf.

[24] Immigration Act 2016, Schedule 10 §2(2).

[25] Home Office, Immigration bail conditions: Electronic Monitoring (EM) expansion pilot Version 2.0, 23 June 2023, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1165035/Immigration_bail_conditions_-_Electronic_Monitoring__EM__Expansion_pilot.pdf.

GPS tags are ankle tags that monitor the location of an individual using satellite and mobile technology,[26] collecting location data (referred to as "trail data") 24 hours a day, 7 days a week, at selected intervals (we know from litigation disclosures that the Home Office uses 30-second collection intervals for all individuals, the most intense frequency available on most tags sold on the market). Trail data is particularly voluminous, sensitive and granular. It provides deep insight into intimate details of an individual's life, revealing a comprehensive picture of everyday habits and movements, permanent or temporary places of residence, hobbies and other activities, social relationships, political, religious or philosophical interests, health concerns, consumption patterns, etc.[27] It is also open to misinterpretation, with different people drawing different conclusions as to an individual's lifestyle. In an immigration enforcement context, this can potentially lead to significant decisions being taken on the basis of subjective interpretations of an individual's movements and activities. Combined with data inaccuracy issues, this can lead the Home Office to make fundamentally wrong assumptions about an individual's movements and activities. Of particular concern, the Home Office plans to use location data collected from GPS tags to inform decisions on individuals' asylum and immigration applications, stating that this will negate the need to request substantiating evidence from third parties.[28] Life-changing and rights-impacting decisions may therefore be made on the basis of this trail data.

Despite the indiscriminate mass nature of this surveillance, there is no provision for judicial or independent oversight at the point where an electronic monitoring condition is imposed by the Home Office.

Testimonies of migrants subjected to GPS tagging collected by PI and other organisations working with migrants in the UK have shown the adverse effects on tagged individuals of permanent live tracking of their location – including constant fear that their movements may trigger a breach alert, anxiety about the tag's battery charge levels when they go out and away from a mains power supply, uncertainty about the interpretation of their movements, or suffering of social

[26] For a technical guide on GPS tracking, see Privacy International, Electronic monitoring using GPS tags: a tech primer, https://privacyinternational.org/explainer/4796/electronic-monitoring-using-gps-tags-tech-primer.

[27] See, for example, jurisprudence of the Court of Justice of the European Union which found: "traffic and location data may reveal information on a significant number of aspects of the private life of the persons concerned, including sensitive information such as sexual orientation, political opinions, religious, philosophical, societal or other beliefs and state of health, given that such data moreover enjoys special protection under EU law. Taken as a whole, that data may allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained, such as the habits of everyday life permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them. In particular, that data provides the means of establishing a profile of the individuals concerned, information that is no less sensitive, having regard to the right to privacy, than the actual content of communications" (6 October 2020, *Joined Cases C-511/18, C-512/18 and C-520/18 La Quadrature du Net and Others v Premier ministre and Others* [2020] ECLI:EU:C:2020:791, para 117.)

[28] See Home Office n 23.

stigma.[29] These adverse effects are entirely disproportionate to the aim pursued (namely to monitor compliance with bail conditions by individuals who are seeking a stable immigration status).

This inevitably leads to a permanent anxiety of going places or making journeys that might later be judged as damaging to their asylum and immigration applications - thereby further impacting their rights to free expression, movement, assembly and association. Because of the significant adverse mental effects on individuals, PI believes that this practice may also amount to cruel, inhuman and degrading treatment, in violation of Article 7 of the ICCPR.

Due to the excessive amounts of data collected, the potential reuses of data, the lack of transparency provided to individuals and the lack of effective oversight, the UK's GPS tagging policy is subject to a number of complaints and lawsuits by tagged individuals.[30] This form of surveillance is a seismic change in the surveillance and control of migrants in the UK. PI is only aware of a similar practice occurring in the United States (and very recently having been rolled out in Australia)[31], a practice that the Human Rights Committee has recently addressed by recommending to increase "the use of alternatives to detention that are respectful of human rights, including the right to privacy, instead of surveillance-based technological alternatives".[32]

3. Surveillance of peaceful assemblies (Article 17 and Article 21)

In the UK, law enforcement agencies develop, acquire, and deploy technologies which have seemingly limitless surveillance capabilities. They have often used them to monitor protests thereby affecting the right to freedom of peaceful assembly as well as the right to privacy of participants.

Research on this topic is hampered by the secrecy surrounding the acquisition and use of these technologies. For example, in 2016, PI submitted freedom of information requests to a number of police forces seeking records related to UK police forces' purchase and use of IMSI catchers.[33]

---

[29] BID, Medical Justice and PLP, Every Move You Make: The Human Cost of GPS Tagging in the Immigration System, October 2022, https://hubble-live-assets.s3.amazonaws.com/biduk/file_asset/file/692/GPS_Tagging_Report_Final__1_.pdf.

[30] See PI complaints to the ICO, 17 August 2022, https://privacyinternational.org/sites/default/files/2022-08/2022.08.17%20-%20Privacy%20International%20complaint%20against%20Home%20Office%20use%20of%20GPS%20Ankle%20Tags%20%5Bpublic%20version%5D.pdf; PI, UK Migrant GPS Tracking Challenges, https://privacyinternational.org/legal-action/uk-migrant-gps-tracking-challenges.

[31] The Guardian, Ankle bracelets, curfews and criminal penalties in Labor response to release of immigration detainees, 15 November 2023, https://www.theguardian.com/australia-news/2023/nov/15/labor-to-fast-track-legislation-to-place-tougher-restrictions-on-released-immigration-detainees.

[32] See Human Rights Committee, Concluding observations on the fifth periodic report of the United States of America, CCPR/C/USA/CO/5, https://tbinternet.ohchr.org/_layouts/15/treatybodyexternal/Download.aspx?symbolno=CCPR%2FC%2FUSA%2FCO%2F5&Lang=en

[33] International Mobile Subscriber Identity catchers (IMSI catchers) can be covertly used to locate and track all mobile phones that are switched on in a certain area. They do this by mimicking a cell-tower and 'enticing' all

The policing bodies refused PI's requests of information on the grounds that they could "neither confirm nor deny" whether they held information responsive to the request, primarily relying on the national security exemption contained in s.24(2) of the Freedom of Information Act. The decision to neither confirm nor deny was further justified in the course of our appeal on the basis that "the deployment of any covert technique or technology is subject to multiple checks and balances to ensure that the rights of the citizenry are protected."[34] Yet this obsessive secrecy, especially with regard to widely known law enforcement techniques, is out of step with the positions of other countries including the United States and Germany.[35] It also leads to inconsistent understanding and application of UK legal frameworks to govern the theoretical use of IMSI catchers as responses to PI by different law enforcement and intelligence authorities have demonstrated.[36]

3.1 Facial recognition technologies

Among the most privacy invasive surveillance technologies deployed by law enforcement agencies in the UK is the use of facial recognition technologies (FRT), which is on the rise in public spaces.

The police have been trialling the use of FRT across the UK as far back as 2016. More recently in May 2023, the Metropolitan Police (the Met) was accused of using King Charles' coronation to stage the biggest live facial recognition operation in British history.[37] In late August 2023, the Ministry of Defence and the Home Office called on companies to "help increase the use and effectiveness of facial recognition technologies within UK policing and security".[38] In September 2023, the Policing Minister, Chris Philip, acknowledged that all 43 UK territorial police forces were now using retrospective FRT, despite previous police denials to this effect.[39] A recent report shows the use of retrospective facial searches conducted by UK police has jumped significantly over the

---

mobile phones within their range to connect to them. IMSI catchers can force those mobile phones to transmit and reveal the phone user's personal details without the user's knowledge. Some IMSI catchers can be used to 'intercept' text messages, calls and internet traffic, allowing whoever is operating the IMSI catcher to read or listen to personal communications. Some IMSI catchers can even re-route or edit communications and data sent to and from our phone and can be used to block service so that phones can no longer be used. See details in Privacy International, "IMSI Catchers: PI's Legal Analysis", June 2020: https://privacyinternational.org/report/3965/imsi-catchers-pis-legal-analysis

[34] PI v Information Commissioner's Office EA/2018/0164/0172, First Tier Tribunal (Information Rights), available online: https://informationrights.decisions.tribunals.gov.uk/DBFiles/Decision/i2576/Privacy%20International%20EA.2018.0164%20(18.02.20).pdfv

[35] See https://privacyinternational.org/long-read/3925/information-tribunal-decisions-re-imsi-catchers-loss-transparency-and-why-we-will .

[36] See https://privacyinternational.org/news-analysis/5206/remember-those-imsi-catchers-uk-authorities-play-hide-and-seek-use-intrusive .

[37] See https://www.theguardian.com/uk-news/2023/may/03/metropolitan-police-live-facial-recognition-in-crowds-at-king-charles-coronation

[38] See https://www.gov.uk/government/publications/facial-recognition/market-exploration-document-facial-recognition

[39] See https://libertyinvestigates.org.uk/articles/hundreds-of-thousands-of-innocent-people-on-police-databases-as-forces-expand-use-of-facial-recognition-tech/

past 5 years. In 2021, 19,827 searches were conducted which jumped to 85,158 searches in 2022.[40]

Despite its widespread deployment, the use of FRT by the police is not adequately regulated in law. 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 laws and equality laws.[41] The case was supported by Liberty and brought by campaigner Ed Bridges, who had his biometric facial data scanned by the FRT on a Cardiff high street in December 2017, and again when he was at a protest in March 2018.[42] The Court agreed that the interference with Article 8 was not in accordance with the law. The Court also found that the Police had not conducted an appropriate Data Protection Impact Assessment in accordance with the Data Protection Act 2018 and that they did not comply with their Public Sector Equality Duty under the Equality Act 2010 to conduct an equality impact assessment.

Yet, the police continue to wrongly justify using FRT through a patchwork of legislation, relying on their common law policing powers and data protection legislation as sufficient in regulating its use. In May 2023, the UK Biometrics and Surveillance Camera Commissioner has critiqued the very limited rules that apply to public space surveillance by the police and noted that oversight and regulation in this area is incomplete, inconsistent and incoherent.[43]

Rather than limiting and properly regulating FRT by law enforcement agencies, the UK government plans to further expand the use of this technology without adequate public scrutiny and consultation. In Clause 21 of the Criminal Justice Bill currently before Parliament,[44] the government is seeking to expand the power of the police to run facial recognition searches on the Driver and Vehicle Licencing Agency (DVLA) database containing images of the UK's 50 million driving licence holders.[45]

4. Recommendations

Based on these observations, Privacy International suggests the Human Rights Committee considers the following recommendations for the UK government:

[40] https://inews.co.uk/news/police-secretive-facial-recognition-database-millions-innocent-people-2635445
[41] See judgment at: https://www.judiciary.uk/wp-content/uploads/2020/08/R-Bridges-v-CC-South-Wales-ors-Judgment.pdf
[42] See https://www.libertyhumanrights.org.uk/issue/liberty-wins-ground-breaking-victory-against-facial-recognition-tech/
[43] See https://videosurveillance.blog.gov.uk/2023/05/17/the-commissioner-discusses-the-new-era-for-live-facial-recognition-after-the-coronation/
[44] See https://publications.parliament.uk/pa/bills/cbill/58-04/0010/230010.pdf
[45] See https://www.theguardian.com/technology/2023/dec/20/police-to-be-able-to-run-face-recognition-searches-on-50m-driving-licence-holders

- Review and reform the IPA 2016 to ensure its compliance with Article 17 of the ICCPR, including by removing the powers of bulk surveillance;

- Abandon efforts to undermine the limited safeguards of the IPA 2016 through the proposed Investigatory Powers Amendment Bill;

- Refrain from taking any measures that undermine or limit the availability of encrypted communications or other important security measures and updates;

- Cease the imposition of GPS tagging on migrants and adopt alternatives to detention that are respectful of human rights, including the right to privacy, instead of surveillance-based technological alternatives;

- Halt and ban the use of live facial recognition technology and ensure that any power to undertake targeted surveillance during protest is transparently regulated and adheres to requirements under international human rights law.