BIG BROTHER WATCH

DEFENDING CIVIL LIBERTIES, PROTECTING PRIVACY

Home Affairs Select Committee: Policing for the Future inquiry

Big Brother Watch – Supplementary evidence

June 2018

CONTENTS

About Big Brother Watch

Big Brother Watch is a cross–party, non-party, independent non-profit organisation leading the protection of privacy and civil liberties in the UK. We expose and challenge threats to people's privacy, freedoms and civil liberties at a time of enormous technological change in the UK.

Summary:

- UK police forces are moving rapidly ahead with the acquisition, development and implementation of new, intrusive and rights-infringing technologies and systems across almost all areas of their work.
- Some of these new technologies may be able to be used in a legal, rights-respecting and safe way with the right safeguards and guidance; however, there are some, such as automated facial recognition, which are so fundamentally dangerous to human rights and democratic freedoms that they should never be used.
- We recommend that the Government takes urgent action to stop, limit, or safeguard a number of new or increasingly prevalent police surveillance technologies and systems which are infringing on individuals' fundamental rights, including automated facial recognition, AI which assists with custody decisions, and software which downloads the contents of people's phones.
- We urge the Committee to look into the vast increase and prevalence of new intrusive technologies being used by the police and to review several of these new technologies and systems being used or trialled by the police for future use.

1. Introduction

1.1 We welcome the opportunity to submit evidence to the *Policing for the Future* inquiry. Due to recent rapid technological advancements leading to new intrusive technologies and systems being used by UK police forces, and the resulting significant implications for the future of policing, we believe it is crucial to draw the Committee's attention to the opportunities and risks at stake.

1.2 Technological developments have been outpacing Government and the law. Police forces are naturally seeking to acquire technology that they believe will improve public safety or save them time and money. However, there is an increasing trend of police forces acquiring, developing, and operationally deploying new, intrusive, and untested technologies that are likely to be incompatible with people's fundamental rights.

1.3 These include new surveillance technologies which indiscriminately track, monitor and identify innocent citizens and their movements; the use of artificial intelligence (AI) and automated systems to predict crime, process individuals in the criminal justice system, and

access and analyse digital evidence; and vast police databases, which include innocent people's images and personal data.

1.4 This submission considers several new technologies and systems being used by the police and their future implications, and draws attention to the increasing tendency of the police to acquire and implement new technologies that engage and sometimes infringe on fundamental rights.

Recommendations

1.5 We call on the Government to:

1.5.1 Immediately end UK police use of automated facial recognition in public spaces in order to prevent unnecessary and disproportionate infringements of the fundamental rights to privacy and freedom of expression and association;

1.5.2 Immediately introduce a policy of automatic deletion of the custody images of unconvicted individuals from police databases, and removes all historic images of unconvicted individuals;

1.5.3 Introduce safeguards in relation to police use of AI, algorithms and other automated systems to protect fundamental rights and prevent the use of AI to make decisions which engage fundamental rights, and restrict the use of predictive policing systems which have the potential to reinforce discriminatory policing;

1.5.4 Review police and CPS guidance, policy and practice in relation to digital evidence, particularly where victims of sexual offences are being re-victimised by intrusive digital investigations, with a view to protecting their Article 8 right to privacy; and

1.5.5 End the indiscriminate tracking and monitoring of UK citizens via the national ANPR network, operating without any legal basis, and remove the historic tracking and location data which is held on the ANPR database.

2. Automated facial recognition in public spaces

2.1 UK police are using automated facial recognition in public spaces and at public events, without any legal basis,[1] policy, or guidance, and it is our view that its use is incompatible with fundamental rights protected by the Human Rights Act 1998.

2.2 South Wales Police used the technology at a lawful and peaceful democratic protest against an arms fair in March 2018, while the Metropolitan Police has targeted people with mental health issues who were not wanted by the police for any crimes at all.

[1] Written parliamentary question answered by Mr Nick Hurd MP on 12 September 2017. (https://www.parliament.uk/business/publications/written-questions-answers-statements/written-question/Commons/2017-09-04/8098/)

2.3 Our investigations and subsequent report, *Face Off: the lawless growth of facial recognition in UK policing,* found that the technology was dangerously inaccurate, with facial recognition cameras misidentifying innocent people up to 98% of the time, with an average of 95% of people misidentified.[2] Both the Metropolitan Police and South Wales Police store images of innocent individuals misidentified by facial recognition for a minimum of 30 days,[3] with South Wales Police informing us they stored them for up to a year.[4] Individuals who are misidentified are not informed of this, and as a result they have no idea that their image has been stored by police

2.4 The technology used by the police has not been tested for potential demographic accuracy biases, despite widespread concerns arising from multiple studies showing that facial recognition technology can disproportionately misidentify people of colour and women.[5]

2.5 However, the legitimacy of this technology does not depend only on its accuracy. It is our analysis that police use of automated facial recognition with public space surveillance cameras is fundamentally contrary to the UK's human rights obligations under the Human Rights Act 1998, specifically the right to privacy, the right to freedom of expression, and the right to freedom of assembly and association.

2.6 Both the police and Government have so far failed to take action to resolve this issue, with the Government consistently stating that this is "an operational matter for the police".[6] As a result, on 14th June 2018 we sent pre-action letters to the Metropolitan Police requesting that they end the use of facial recognition, and the Home Secretary, requesting that he withdraw support for the technology. If they continue to use facial recognition surveillance, we will challenge its legality in court.[7] **Big Brother Watch urges the Government to immediately stop police using automated facial recognition with public surveillance cameras.**

---

[2] Big Brother Watch (2018), 'Face Off: the lawless growth of facial recognition in UK policing', 15th May 2018 (https://bigbrotherwatch.org.uk/wp-content/uploads/2018/05/Face-Off-final-digital-1.pdf)

[3] Metropolitan Police, 'Freedom of Information Request' (https://bigbrotherwatch.org.uk/wp-content/uploads/2018/04/Metropolitan-Police-2018030000340.pdf)

[4] South Wales police, 'Freedom of Information Request', 27th March 2018 (https://bigbrotherwatch.org.uk/wp-content/uploads/2018/04/Response-287_18.pdf)

[5] Buolamwini, Joy; Gebru, Timmit: Gender Shades – Intersectional Accuracy Disparities in Commercial Gender Classification. In: Proceedings of Machine Learning Research 81:1, p.1-15, 2018. (http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf)
The study analysed the software made by Microsoft, IBM and Face++, which provides its software to the Chinese government.

[6] Layla Moran, Written Parliamentary Question, 4th May 2018 (https://www.parliament.uk/business/publications/written-questions-answers-statements/written-question/Commons/2018-05-04/141377/)

[7] https://bigbrotherwatch.org.uk/all-media/big-brother-watch-launches-legal-challenge-to-government-and-met-police-on-dangerously-authoritarian-facial-recognition-cameras/

3. Custody images, static facial recognition and biometrics

3.1 There around 19 million custody images on the Police National Database.[8] A staggering 12.5million of these images have been made biometrically searchable by facial recognition technology, following an upgrade to the system in 2014 which occurred without parliamentary or public scrutiny.[9]

3.2 However, many people who have a custody image taken are either never charged or are found not guilty. It has been estimated by the Biometrics Commissioner that hundreds of thousands of images on the Police National Database are of innocent people.[10]

3.3 The High Court ruled in 2012 that the indefinite retention of innocent people's custody images was "unlawful";[11] however, neither the Home Office nor the police have taken any action to resolve this. The Home Office created a policy in 2017 whereby innocent people can write to their local police force to request the deletion of their custody image.[12] This new policy was exposed as a failure by a Press Association investigation which revealed only 67 applications had been made, and only 34 had been successful.[13] Norman Lamb MP, Chair of the Science and Technology Committee, publicly voiced his concerns that the Home Office's retention and deletion- policies are likely to be unlawful.[14]

3.4 The Home Office has claimed that there would be prohibitive costs involved in deleting innocent peoples images.[15] However, at the same time, the Home Office has awarded millions in funding to police to implement automated facial recognition – including £2.6million to South Wales Police.[16]

3.5 With sub-sets of this database being used at police deployments of automated facial recognition, innocent people are increasingly at risk of being wrongfully stopped or even arrested. This also completely blurs the line between the innocent and the guilty, and makes a mockery of the presumption of innocence.

---

[8] Press Association: 'Custody image' deletion request figures revealed, 12 February 2018 (http://www.dailymail.co.uk/wires/pa/article-5379353/Custody-image-deletion-request-figures-revealed.htm)

[9] Science and Technology Committee: Oral Evidence – Biometrics Strategy and Forensic Services, HC 800, 6 February 2018. (http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/science-and-technology-committee/biometrics-strategy-and-forensic-services/oral/78113.htm)

[10] BBC News Online, 'Facial recognition database 'risks targeting innocent people', 14 September 2018 (http://www.bbc.co.uk/news/uk-41262064)

[11] *RMC and FJ v Commissioner of Police for the Metropolis and Secretary of State for the Home Department* [2012] EWHC 1681 (Admin)

[12] Home Office, 'Review of the Use and Retention of Custody Images', February 2017 (https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/594463/2017-02-23_Custody_Image_Review.pdf)

[13] Press Association: 'Custody image' deletion request figures revealed, 12 February 2018 (http://www.dailymail.co.uk/wires/pa/article-5379353/Custody-image-deletion-request-figures-revealed.htm)

[14] Daily Mail, 'Arrangements for storing millions of 'custody images' may be unlawful, MP says' 14 February 2018 (http://www.dailymail.co.uk/wires/pa/article-5389875/Arrangements-storing-millions-custody-images-unlawful-MP-says.html)

[15] The Independent, ''Too expensive' to delete millions of police mugshots of innocent people, minister claims' 19 April 2018 (https://www.independent.co.uk/news/uk/politics/police-mugshots-innocent-people-cant-delete-expensive-mp-committee-high-court-ruling-a8310896.html)

[16] South Wales Police and Crime Commissioner, Medium Term Financial Strategy2017-2021 (https://pcclivewww.blob.core.windows.net/wordpress-uploads/2016-12-28-Final-Medium-Term-Financial-Strategy.pdf)

3.6 The Science and Technology Committee recently reported that the Government's current approach was "unacceptable", and urged the Government to introduce a "comprehensive deletion system as a matter of urgency".[17]

3.7 **Big Brother Watch urges the Government to immediately introduce a policy of automatic deletion of innocent people's custody images from police databases and remove all historic images of unconvicted people from police databases.**

4. Police artificial intelligence and automated decision-making systems

4.1 A number of UK police forces are using or plan to use AI, machine-learning algorithms or other automated systems as part of their work.

4.2 Durham Police has developed a machine learning algorithm called the Harm Assessment Risk Tool (HART) which scores a suspect's risk of re-offending in the future. This AI-generated risk score is used to advise whether to charge a suspect or release them onto a rehabilitation programme.

4.3 One of the data sources fed into the HART system is global data broker Experian's 'Mosaic' tool – postcode stereotypes built from commercial marketing data. The 850 million pieces of data used to create these stereotypes include health data, GCSE results, child benefits and income support, family and personal names linked to ethnicity, data scraped from online sources and much more.

4.4 This data profiles all 50 million adults in the UK[18] into stereotypes based on their postcodes, creating profiles such as "Asian Heritage" or "Disconnected Youth".[19] Experian's profiles attribute 'demographic characteristics' to each stereotype – characterising "Asian Heritage" as "extended families" living in "inexpensive, close-packed Victorian terraces", adding that "when people do have jobs, they are generally in low paid routine occupations in transport or food service".[20] It is appalling that this kind of profiling and stereotyping data is being used by police AI systems to predict people's supposed "risk", with the potential of affecting potentially life-changing criminal justice decisions. Allowing this kind of profiling data to be used will inevitably lead to unfair and inaccurate decisions, and a 'postcode lottery' of justice, reinforcing existing biases and inequality.

---

[17] HoC Science and Technology Committee, ' Biometrics strategy and forensic services" 23 May 2018 (https://publications.parliament.uk/pa/cm201719/cmselect/cmsctech/800/800.pdf)

[18] Mosaic Infographic, Experian, (http://www.experian.co.uk/marketing-services/knowledge/infographics/infographic-new-mosaic.html) Also see Paul Cresswell et al, 'Under the bonnet: Mosaic data, methodology and build', Experian Marketing Services, 1 April 2014, p.7: (http://www.experian.co.uk/assets/marketing-services/presentations/mosaic-data-methodology-and-build.pdf)

[19] Mosaic Public Sector brochure, Experian, 2016, pp.6-9: (http://www.experian.co.uk/assets/marketing-services/brochures/mosaic-ps-brochure.pdf)

[20] Mosaic UK Data Profile, Experian, 2017, p.51: (https://www.experianintact.com/content/uk/documents/productSheets/MosaicConsumerUK.pdf)

4.5 Meanwhile, Kent Police has been using commercial 'predictive policing' software called PredPol since 2013,[21] while similar systems have been trialled by Greater Manchester, West Midlands, Yorkshire and the Metropolitan Police.[22] The system uses historic geographic crime information to predict geographical areas where crime is likely to be committed. Multiple studies and reports have found that such systems can reinforce existing patterns of discrimination and result in feedback loops, where police are repeatedly sent back to the same over-policed neighbourhoods regardless of the actual crime rate. [23]

4.6 It has also recently been reported that the police are trialling the use of AI to analyse digital evidence.[24] We are extremely concerned that such sensitive police work is being outsourced to experimental systems, with little or no consideration of the myriad transparency, accountability and privacy issues involved, such as the victim of a sexual offence having their digital life put on trial by a faceless AI system. The issue of police access to and analysis of digital evidence is considered in more detail below.

4.7 The recently passed Data Protection Act 2018 allows derogations from the right not to be subject to an automated decision set out in the GDPR.[25] This means that UK police are allowed by law to subject individuals to purely automated decisions that engage and affect people's rights. For example, it would permit Durham Police's HART system to not only influence decisions but to actually make decisions about risk and prosecution. Big Brother Watch campaigned for amendments to the Data Protection Bill which would have ensured human decisions were ultimately required where any automated decision-making systems engage human rights.[26] Our amendments were tabled at Committee stage and Report stage, but were narrowly defeated by the Government. Our full briefing on the (then) Bill is available on our website.[27]

4.8 **Big Brother Watch recommends that the Government introduces human rights safeguards in relation to UK police use of AI, algorithmic decision-making systems and other automated systems that engage fundamental rights; and restricts the use of predictive policing systems which have the potential to reinforce discriminatory policing.**

---

[21] https://www.independent.co.uk/news/uk/home-news/police-big-data-technology-predict-crime-hotspot-mapping-rusi-report-research-minority-report-a7963706.html

[22] https://www.ibtimes.co.uk/predictive-policing-predpol-future-crime-509891

[23] Ensign et al, (2017) 'Runaway Feedback Loops in Predictive Policing', Cornell University Library, 29 June 2019 https://arxiv.org/abs/1706.0984)

[24] https://www.theguardian.com/uk-news/2018/may/27/police-trial-ai-software-to-help-process-mobile-phone-evidence

[25] Data Protection Act 2018, Section 49(1)

[26] Big Brother Watch, 'Big Brother Watch's Briefing on the Data Protection Bill for Committee Stage in the House of Commons', March 2018 (https://bigbrotherwatch.org.uk/wp-content/uploads/2018/03/Big-Brother-Watch%E2%80%99s-Briefing-on-the-Data-Protection-Bill-for-Committee-Stage-in-the-House-of-Commons.pdf)
See also: Griff Ferris, "We Must Protect Our Rights From Automated Decisions", The Huffington Post, 14 March 2018 (https://www.huffingtonpost.co.uk/entry/the-future-is-now-we-must-protect-our-rights-from_uk_5aa91fb5e4b0dccc83c1ed5b)

[27] Big Brother Watch, 'Big Brother Watch's Briefing on the Data Protection Bill for Committee Stage in the House of Commons', March 2018 (https://bigbrotherwatch.org.uk/wp-content/uploads/2018/03/Big-Brother-Watch%E2%80%99s-Briefing-on-the-Data-Protection-Bill-for-Committee-Stage-in-the-House-of-Commons.pdf)

5. Digital evidence and disclosure in sexual offences cases

5.1 Digital evidence is unsurprisingly a key part of an increasing number of criminal investigations. Our investigation into police use of digital evidence in November 2017 found that 93% of police forces were extracting data from digital devices including mobile phones, laptops, tablets and computers.[28] Police are using more and more advanced technology to access, download, and analyse digital evidence as part of these investigations.[29] While it is inevitable that the police need to engage with digital information, we are concerned about the extremely intrusive, incoherent and potentially rights-infringing way in which this is currently being done.

5.2 There has been much focus, and rightly so, on the issue of disclosure of digital evidence in sexual offences case, and the Justice Committee's current inquiry has specifically looked at the implications for the growth in volume of digital evidence.[30] However, there has been a disproportionate focus in the media on alleged perpetrators of sexual offences and the potential miscarriages of justice that have occurred or almost occurred to these individuals, supposedly as a result of insufficient disclosure of digital evidence, as opposed to the lack of justice for victims of sexual offences and the digital evidence issues they also face.

5.3 We are concerned about the access, collection, analysis, and disclosure of digital evidence in relation to victims of sexual offences, and the potential infringement of their Article 8 right to privacy in the disclosure process.

5.4 Victims of crime typically supply evidence that is relevant to the crime that has taken place. It is rare that the integrity of such evidence is, by default, put under such scrutiny as it is where victims of rape and sexual offences are concerned.

5.5 Victims of rape and sexual offences are being re-victimised in the investigation process as the entire contents of their phones and digital devices are accessed and downloaded, and their digital lives and information are subject to intense scrutiny and investigation. Police are also requesting access via logins and passwords to victims' personal 'cloud' storage services and social media accounts.

5.6 Dame Vera Baird QC, Policing and Crime Commissioner for Northumbria and the lead for supporting victims for the Association of Police and Crime Commissioners (APCC), has warned:

> *"...we need to ensure that complainants are not discouraged from coming forward to report sexual offences by inappropriate 'fishing' into personal records, access to which is demanded in no other kind of case."*

---

[28] Big Brother Watch, 'Police Access to Digital Evidence', November 2017 (https://bigbrotherwatch.org.uk/wp-content/uploads/2017/11/Police-Access-to-Digital-Evidence-1.pdf)

[29] Privacy International, 'Digital Stop and Search', 27 March 2018 (https://privacyinternational.org/report/1699/digital-stop-and-search-how-uk-police-can-secretly-download-everything-your-mobile)

[30] Disclosure of evidence in criminal cases inquiry: https://www.parliament.uk/business/committees/committees-a-z/commons-select/justice-committee/inquiries/parliament-2017/disclosure-criminal-cases-17-19/

5.7 Furthermore, the Crown Prosecution Service (CPS) "require police to gather third party material [on victims of sexual offences] from healthcare providers, including psychiatric records, from social services and educational establishments, from counsellors and from family court proceedings. Unless this is done, the CPS will not consider a charge."[31]

5.8 We are concerned about current disclosure practices and disproportionate infringements of victims' Article 8 right to privacy, particularly in light of the extensive amount of sensitive material about a victim which the CPS requires before it will consider a charge. This includes the use of 'Stafford statements',[32] where victims of sexual offences are encouraged to consent to disclosure of evidence relating to them, including the above 'third party material'. This follows from the case of *R (B) v Stafford Crown Court* [2007], which held that in sexual offences cases, a victim's Article 8 right to privacy must be taken into account regarding the disclosure of evidence relating to them, for example psychiatric or medical records, and the victim must be given proper notice and the allowed the opportunity to make representations on the proposed disclosure.[33]

5.9 However, if consent is given via one of these statements, it allows the disclosure of all or any of the potentially extremely sensitive 'third party material' such as psychiatric and educational records, as well as doing away with the requirement for a hearing to consider the victims Article 8 rights, and preventing the victim from airing their concerns about the disclosure at such a hearing. At the very least, the apparent reluctance of the CPS to consider a charge unless they have available such a broad range of extremely sensitive and personal information appears to be a disproportionate practice which ignores a victim's Article 8 right. Moreover, this also puts undue pressure on the victim to consent to the disclosure.

5.10 Also concerning is the way that these 'Stafford' statements are presented to the victim as an additional witness statement (indeed, a copy of such a statement seen by Big Brother Watch was marked 'Witness Statement') or a 'consent form', and Dame Vera Baird QC has expressed fears they may not be read thoroughly, resulting in victims unknowingly restricting their ability to exercise their Article 8 rights.[34]

5.11 This is completely at odds with the treatment of the defendant, who is not put under any such obligation to reveal such information or material in relation to their own circumstances, other than to give a 'defence statement'.[35]

---

[31] Dame Vera Baird QC, PCC for Northumbria, 'Letter to Justice Committee', 14 February 2018 (http://www.apccs.police.uk/wp-content/uploads/2016/11/Letter-to-Justice-Committee-Chair-regarding-disclosure-in-criminal-cases-140218.pdf)

[32] Following *R (B) v Stafford Crown Court* [2007] 1 All ER, a complainant's Article 8 rights must be considered when it comes to disclosure.

[33] This is also now set out in Part 28 of the Criminal Procedure Rules 2010

[34] Dame Vera Baird QC, PCC for Northumbria, 'Letter to Justice Committee', 14 February 2018 (http://www.apccs.police.uk/wp-content/uploads/2016/11/Letter-to-Justice-Committee-Chair-regarding-disclosure-in-criminal-cases-140218.pdf)

[35] Criminal Procedure and Investigations Act 1996, s5(5)

5.12 Not only is it a significant concern that victims of sexual offences are being subject to such intense and invasive scrutiny of extremely sensitive and personal elements of their lives to the point where they themselves are put under investigation, but that they may not be fully aware of the extent to which they are consenting to disclosure of this information in court, and may even be put under pressure to consent to such disclosure. This invasion of a victim's privacy, through the access to and collection of vast and unnecessary amounts of digital evidence as well as 'third party material', is disproportionate.

5.13 This has the unsurprising but extremely significant effect that many victims are unwilling to come forward, or withdraw their cases when faced with such intrusion into their private life.

5.14 Recent reports that police are now trialling the use of artificial intelligence (AI) to trawl through digital evidence, including that of victims of sexual offences, is extremely concerning.[36] The police should not be outsourcing such extremely sensitive tasks to an experimental computer system that obstructs accountability and transparency. This could allow for even more disproportionate intrusions of privacy, with the software being trialled by the Metropolitan Police allowing the police to "visualise social networks" and "enable images and videos to be tagged as to whether the content includes…nudity". [37]

5.15 In addition, we are concerned about the lack of up to date policy in this area, particularly with regards to police practices, and the lack of guidance and safeguards to prevent police from downloading and analysing the entire digital contents of a victim's phone, tablet and laptop, and requiring logins and passwords to personal data storage or 'cloud' services and social media accounts, as a matter of course.[38] The most up-to-date policy and 'good practice' guidance available to police to guide their access to digital evidence is the Association of Chief Police Officers (ACPO) *ACPO Good Practice Guide for Digital Evidence* – published in March 2012, over 6 years ago.[39] Meanwhile, the Crown Prosecution Service's *Policy for Prosecuting Cases of Rape* was last updated in 2012.[40] The NPCC and CPS themselves have commented that the two most significant guiding factors in relation to disclosure of evidence, the Criminal Procedures and Investigations Act (CPIA) 1996, and the 2013 Attorney General's Guidelines "were not designed with the sheer volume of digital unused material that is now common to (…) crime cases."[41]

5.16 We have further concerns about the lack of expert and sensitive training within the police to deal with the technical aspects of digital evidence. Her Majesty's Chief Inspector of

---

[36] https://www.theguardian.com/uk-news/2018/may/27/police-trial-ai-software-to-help-process-mobile-phone-evidence

[37] https://www.theguardian.com/uk-news/2018/may/27/police-trial-ai-software-to-help-process-mobile-phone-evidence

[38] Angiolini Review, 2015, Para 418, 419, 421 (https://www.cps.gov.uk/sites/default/files/documents/publications/dame_elish_angiolini_rape_review_2015.pdf)

[39] ACPO, 'ACPO Good Practice Guide for Digital Evidence' March 2012 (http://library.college.police.uk/docs/acpo/digital-evidence-2012.pdf)

[40] CPS, 'CPS Policy for Prosecuting Cases of Rape', September 2012 (Available: https://www.cps.gov.uk/publication/cps-policy-prosecuting-cases-rape)

[41] NPCC and CPS, 'Written Evidence to the Justice Committee', 24 April 2018 Para 25 (http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/justice-committee/disclosure-of-evidence-in-criminal-cases/written/80778.html)

Constabulary's (HMIC) 2016 report on the state of policing found that police forces were being "overwhelmed" by digital evidence, and that "forces urgently need to recruit and train a workforce that is fit for a digital future".[42] Another HMIC report in 2015 found that police officers themselves felt "frustrated with their lack of ability to deal with digital investigations".[43]

5.17 **Big Brother Watch recommends that the Government urgently reviews and updates current police guidance, policy, and practices, and Crown Prosecution Service guidance, policy, and practices, in relation to the collection and examination of digital evidence in sexual offences cases, and ends the disproportionate intrusion of privacy suffered by victims of sexual offences.**

6. ANPR

6.1 Automated Number Plate Recognition (ANPR) cameras now make up a national surveillance framework across the country, tracking and storing people's locations. They have dramatically increased from 2,000 cameras in 2006[44] to 9,000 in 2017.[45] These cameras scan 25 to 40 million car number plates every day across UK roads, and this data is stored for 12 months. This has created, according to the Surveillance Camera Commissioner, "one of the largest non military databases in the UK", holding "up to 20 billion records".[46]

6.2 ANPR is a prime example of the creeping use of surveillance technologies by the police. This system was introduced in the UK in the late 1970's and has grown exponentially over the last 40 years into the surveillance and location tracking network it is today. The SCC has noted that "Law enforcement ANPR in the UK must surely be one of the largest data gatherers of its citizens in the world".[47]

6.3 There is no legal basis for the use of ANPR or the retention of this location data and its use has never been agreed by parliament. This was noted by the Surveillance Camera Commissioner in 2015:

---

[42] HMIC, 'State of Policing 2016, (Published 2017) Pg 24 (https://www.justiceinspectorates.gov.uk/hmicfrs/wp-content/uploads/state-of-policing-2016.pdf)
[43] HMIC, 'Real Lives, real crimes: a study of digital crime and policing, December 2015 (https://www.justiceinspectorates.gov.uk/hmicfrs/wp-content/uploads/real-lives-real-crimes-a-study-of-digital-crime-and-policing.pdf)
[44] The Guardian: https://www.theguardian.com/uk-news/2014/jan/23/anpr-automated-numberplate-recognition-cameras
[45] Surveillance Camera Commissioner, *Annual Report 2016/17,* January 2018 (https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/672286/CCS207_CCS0118716124-1_Annex_A_-_AR_2017-_web.pdf)
[46] Surveillance Camera Commissioner, *Annual Report 2016/17,* January 2018 (https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/672286/CCS207_CCS0118716124-1_Annex_A_-_AR_2017-_web.pdf)
[47] Surveillance Camera Commissioner, *Annual Report 2016/17,* January 2018 (https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/672286/CCS207_CCS0118716124-1_Annex_A_-_AR_2017-_web.pdf)

"There is no statutory authority for the creation of the national ANPR database, its creation was never agreed by parliament, and no report on its operation has even been laid before parliament."[48]

6.4 Recent jurisprudence by the European Court of Justice[49] and the European Court of Human Rights[50] also suggests that this collection and retention of location data may be incompatible with Article 7 and Article 8 of the EU Charter of Fundamental Rights and or Article 8 of the European Convention on Human Rights.

6.5 **Big Brother Watch urges the Government to end the indiscriminate tracking and monitoring of UK citizens via the national ANPR network as well as the retention of 12 months of location data.**

7. National law Enforcement Data Service (NLEDS)

7.1 UK police forces, under the auspices of the Home Office, plan to create a huge integrated database of all police information, hosted on a cloud service provided by Amazon Web Services: the National law Enforcement Data Service (NLEDS).

7.2 The Home Office has tendered for an application to access this cloud database,[51] which would "run on hand-held devices", "for police officers actually in their cars".[52]

7.3 This could allow an unprecedented and disproportionate amount of information to be available to a front-line police officer. The availability and vulnerability of such information from a front-line device opens up the possibility for data loss, hacking, or abuse.

7.4 This application would be searchable by "authorised Agencies" which would include "Border Control / Immigration" and unspecified "Government Departments" and "Government Agencies", who could "check an individual's identity, offending history, status, and location, to "analyse data to identify links between people, objects, locations and events", and to "set up automated alerts for new or changed data and events of interest".[53] This would appear to allow government departments unprecedented access to sensitive information about individuals who have come into contact with the police and the criminal justice system.

---

[48] Surveillance Camera Commissioner, *Annual Report 2015/16*, 16th November 2016, p. 23: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/569559/57586_unnum_camera_WEB.PDF

[49] Joined Cases C-203/15 *Tele2* Sverige AB v Post-och telestyrelsen and C-698/15 SSHD v Tom *Watson* & Others.

[50] *Taylor-Sabori v United Kingdom*: ECHR 22 Oct 2002; *Uzun v Germany* (Application no. 35623/05), 2 December 2010;

[51] Gov.uk Digital Marketplace, 'Home Office (HO) National Law Enforcement Data Programme (NLEDP) Application Development Service (https://www.digitalmarketplace.service.gov.uk/digital-outcomes-and-specialists/opportunities/1227)

[52] The Register, 'UK Home Office is creating mega database by stitching together ALL its gov records' 3 June 2016 (https://www.theregister.co.uk/2016/06/03/home_office_mega_database/)

[53] Government Digital Marketplace, Home Office (HO) National Law Enforcement Data Programme (NLEDP) Application Development Service (https://www.digitalmarketplace.service.gov.uk/digital-outcomes-and-specialists/opportunities/1227

Further, there is also the intention that the application "can run analytics" and all sorts of various algorithms… including machine learning".

7.5 The draft Privacy Impact Assessment (PIA) given to us by the Home Office stated that NLEDS will also allow a "facial search" of images on the service. The PIA notes that NLEDS may retain "arrest data (not charged or not convicted), charging data (not convicted) or very minor historical conviction data".

7.6 There has been no consideration of this new system by Parliament. Whilst modernised policing systems are welcome, there needs to be significant and meaningful consideration of the privacy issues involved in such a large database of personal information, the access to such a database via an application available to all police officers, and the use of machine-learning algorithms in the criminal justice system.

8. Conclusion

8.1 The police are currently able to acquire, develop and implement new intrusive surveillance, identification and tracking technologies; predictive policing systems; to intrude into people's private lives with advanced data access and analysis technology; and to create vast interlinked databases, without any parliamentary or public scrutiny, or serious consideration of their compatibility with fundamental rights.

8.2 As considered in this submission, there is an increasing trend for the implementation of new technologies that interfere with fundamental rights. The current approach by police towards the introduction and operational deployment of new technologies often completely disregards fundamental rights in favour of technological possibility. Current law, such as the Protection of Freedoms Act 2012, and safeguards, such as requirements for Data Protection Impact Assessments and/or Privacy Impact Assessments as part of such an implementation, have not prevented this. In the context of facial recognition, for example, the Surveillance Camera Commissioner has stated:

> "As new technology becomes available or widely used how do we ensure that it is used within the legislative framework – for example under what legislative footing is automatic facial recognition?".[54]

8.3 The Biometrics Commissioner states his proposed solution in his annual report for 2017 (published June 2018):

> "The police service needs to agree a common framework for the development, testing, evaluation and mutual implementation of new technologies. This is necessary if the service is going to keep ahead of new technology and be in a position to decide, on the basis of empirical evidence, how useful a particular

[54] Surveillance Camera Commissioner, 'A National Surveillance Camera Strategy for England and Wales', March 2017, para. 35, p.12

technology will be for policing and, additionally, whether national deployment is in the public interest and is cost-effective." [55]

8.4 We would add that any new policing technology which impacts members should have its impact on fundamental rights considered, specifically its compatibility with the existing human rights framework in the UK. In this context, the Biometrics Commissioner also noted:

> "Whilst the state may have powerful new tools available to it, if misused, they could undermine the very liberties and civil society that it is seeking to protect."[56]

8.5 **We urge the Committee to look into the vast increase and prevalence of new intrusive surveillance technologies being used by the police, and consider the powers or lack of oversight that enable the police to adopt new technologies, such as ANPR or automated facial recognition, unilaterally.**

Griff Ferris

Legal and Policy officer

Big Brother Watch

[55] Commissioner for the Use and Retention of Biometric Material (Paul Wiles), 'Annual Report 2017', March 2018 (Published 5th June 2018), Para 311
[56] Ibid, para 298