Submission to the Justice and Home Affairs Committee Inquiry: New technologies and the application of the law — defend digital me

About defenddigitalme

defenddigitalme is a call to action to protect children's rights to privacy. We are teachers and parents who campaign for safe, fair and transparent data processing in education, in England, and beyond. Founded in 2017 as a not for profit organisation, we are funded by the Joseph Rowntree Charitable Trust.

We specialise in children's and learner records across the public sector. Since the Department for Education (DfE) began giving police access to children's records from the 28 million named learner records and the national pupil database we have taken a further interest in use by law enforcement.

Jen Persson (Director) has attended an ongoing series of discussions since 2018 between the Royal College of Policing, the Home Office, their Biometrics working group, police staff, the Information Commissioner's Office, and various third sector organisations. The *Open Space*[1] workshops facilitated by *Involve*, focus on the National Law Enforcement Database[2] (NLEDS), but also integrating Immigration Databases and use of Biometrics (HOB). The use of emerging technology in policing is changing how policing operates, and police interactions with individuals and communities in opaque ways, and with potentially profound effects for society— the committee inquiry on emerging technology is both timely and urgent.

We draw the attention of the Committee to three relevant publications in September 2021:

- Government's proposals to reform the UK data protection law: Data: A new direction
- The National Audit Office: The National Law Enforcement Data Programme report
- PPO Ombudsman independent investigation into death of a baby at HMP Bronzefield

1. Emerging technologies used in policing children in practice

1. In a submission to the College of Policing Code of Practice consultation on use of data earlier this year, defenddigitalme raised issues to highlight that existing Codes of Practice on data and information use, are not fit for purpose when it comes to emerging technologies.[3]

2. The West Midlands Police Ethics Committee[4] has also expressed concerns with regard to the applied uses of emerging technologies used in policing children. We are not aware of other forces that have similar models of challenge, but others already use similar tools.

3. Emerging technologies can mean interventions are made that affect communities and individuals' lives and decisions taken on how to allocate resources. The remoteness of many tools enable the opaque and unseen policing of individuals at scale who are in public spaces

---

[1] How can civil society be involved in shaping law enforcement data and biometrics programmes?
https://www.involve.org.uk/our-work/our-projects/practice/how-can-civil-society-be-involved-shaping-law-enforcement-data
[2] The National Audit Office (September 2021) National Law Enforcement Data Programme
https://www.nao.org.uk/press-release/the-national-law-enforcement-data-programme/
[3] defenddigitalme submission to the College of Policing Public consultation: a new Code of Practice for information and records management (consultation page https://www.college.police.uk/article/information-records-management-consultation)
https://defenddigitalme.org/wp-content/uploads/2021/03/Consultation-PCOC-2021-DDM-v1.0.pdf
[4] 14122020 - EC - Agenda Item 3c - Analysis of school catchment areas and violence – proposal
https://www.westmidlands-pcc.gov.uk/wp-content/uploads/2021/02/14122020-EC-Minutes-Advice.pdf?x86491

without being under any suspicion of criminality (e.g. live facial recognition, drones, IMSI catchers[5]). New technology may pose new state threats. Data analytics may be used at speed and scale to make inferences based on historical data or identify patterns and 'hot spots' on which interventions are based with today's population including children. Black young people are overly represented in stop and search.The technology is already available for checking fingerprints at the side of the street[6] but what oversight with regard to children? Procurement proceeds with a deficit in parliamentary scrutiny or public democratic debate.[7]

4. The technology choices being made across the whole of the justice system may appear contradictory. To give one example, in stark contrast to what appear to be unlimited proposals that expand the use of technology for surveillance or in predictive policing, there appear to be none proposed for the care of expectant mothers and their child-at-risk in [HMP Bronzefield] prison.[8]

5. Transparency and scrutiny are needed if the overall tangible and intangible costs of both lack of investment or of procurement are to be assessed and made available and accountable to the public. Consistent transparency reporting of the adoption and application of technology could be made via Police and Crime Commissioner (PCC) annual reports. It might include for example, registers of algorithms and the application of automated data analytics, as well as standardised metrics for reporting sourcing and spending. This could contribute to building trustworthy analysis of the changing environment.

2. Background on children, data and policing

6. The children of today are growing up in a policing environment that is ever more datafied, quantified, and seen through the lens of a computer analysis, out of context. Children are rapidly given binary labels in systems out of context; offenders, victims or criminals.[9] This emerging environment is rarely well understood by parliamentarians in our experience.[10]

7.Children are disadvantaged in a world that is ever more mechanistic and automated. Disproportionate harm may be felt by children including those from marginalised communities in processes that fail to take into account the nature of human beings. Children are developing into adulthood, and need particular consideration according to their capacity and recognition of their lack of agency and disempowerment in relationship with authority.

8. Who is a child? Anyone under the age of 18 is regarded as a child under the UN Convention on the Rights of the Child. The UK supports unusually young ages of criminal responsibility, in conflict with the UNCRC recommendations. In Scotland the age was raised

---

[5] More UK Police Put Cash Down for IMSI Catchers
 (2017) https://www.vice.com/en/article/7xz5pq/more-uk-police-put-cash-down-for-imsi-catchers
[6] https://www.wired.co.uk/article/uk-police-handheld-fingerprint-scanner-database-biometric-security
[7] Oldham, J (2021) Concern at West Midlands Police proposals to use crime data to identify young 'violent offenders' in school catchment areas (Birmingham Mail)
https://www.birminghammail.co.uk/news/midlands-news/fears-over-police-plan-identify-20193614
[8] PPO Ombudsman independent investigation into tragic death of a baby at HMP Bronzefield (September 2021)
https://www.ppo.gov.uk/news/ppo-ombudsman-sue-mcallister-publishes-independent-investigation-into-the-tragic-death-of-a-baby-at-hmp-bronzefield/
[9] A member of the West Midlands Ethics Committee in December 2020 expressed discomfort with some of the language used in the WMP report, and proposed changing the language to children and young people as opposed to offenders, and noted it could be, worryingly, described as violent offences committed by children. 14122020 - EC - Minutes Advice
https://www.westmidlands-pcc.gov.uk/ethics-committee/ethics-committee-reports-and-minutes/
[10] defenddigitalme briefing on the Police, Crime, Sentencing and Courts (PCSC) Bill
https://defenddigitalme.org/2021/05/the-police-crime-sentencing-and-courts-pcsc-bill-briefing

to 12 in 2019, whereas England remains behind at age 10. In regards to the adoption of technology there is no overarching Code of Practice when it comes to child justice and policing, such as might uphold the principles set out in the UNCRC General Comment no.10 Children's rights in juvenile justice (2007)[11]. Our proposals for a child rights impact assessment of NLEDS have not been accepted or operationalised.

9. Who "the police" includes, is changing rapidly with the collaboration across private providers and access by police to tools such as Amazon Ring, or to supermarket loyalty card records, commercial data brokers, and surveillance of social media and wider data sources. There is direct police presence in schools, and there is widespread use of equipment for the indirect policing of behaviour that may be shared with law enforcement, such as CCTV, bodycams, biometrics and digital monitoring in schools. Immigration enforcement is increasingly conflated with law enforcement. In practical terms this increases data access such as the repurposing of school records for the purposes of the Hostile Environment.

10. *How* the police operate is changing rapidly using technology and with little consistent approach to scrutiny or oversight. The NAO audit of the NLEDS found that "in autumn 2020 the police lost confidence in the programme". "The "mega-database" was intended to replace the Police National Computer (PNC) and the Police National Database (PND), as well as take copies of all DVLA records, and include immigration databases. All access will be enabled through a common front-end, user interface. Original plans have changed.

11. What is "the data" talked about used in policing? Data come from a vast number of sources. Retrospective data management good practice tends to be seen as a burden, despite institutional obligations across the data lifecycle.*"The volume of data is going up and up..."[12] "We've got so much of that information, how do we start to manage it." "How do we know what information we've got."* (Phil Tomlinson, Head of Digital Intelligence, Met. Police)

12. Police actions are guided by Codes of Practice that are out of date and unfit for purpose in the digital environment. Our March 2021 submission to the Police consultation on a Code of Practice for Information and Records Management highlights some of our reasoning why. New Codes of practice fail to address well-known data related issues that have not met ethical or lawful standards in the past. Case studies include:

   a. Abuse of deceased children's personal data and identities by undercover police.[13]
   b. The Gangs' Matrix[14] that "does not clearly distinguish between the approach to victims of gang-related crime and the perpetrators, leading to confusion amongst those using it, or serious breaches of data protection laws with the potential to cause damage and distress to the disproportionate number of young, black men".
   c. Failure to communicate rights on informed processing and Subject Access duties.[15]

---

[11] General comment No. 10 (2007): Children's Rights in Juvenile Justice
https://www.refworld.org/publisher,CRC,GENERAL,,4670fca12,0.html
[12] Phil Tomlinson, Head of Digital Intelligence, Metropolitan Police (September 22, 2021)
https://data.govx.digital/talks/managing-the-government-data-lifecycle/
[13] The Guardian (2020) Met faces legal action over spies' use of dead children's identities
https://www.theguardian.com/uk-news/2020/dec/07/met-police-legal-action-spies-use-dead-childrens-identities
[14] The ICO (2018) ICO finds Metropolitan Police Service's Gangs Matrix breached data protection laws
https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2018/11/ico-finds-metropolitan-police-service-s-gangs-matrix-breached-data-protection-laws/
[15] The ICO (June 2019) Enforcement notices served against the Met Police Service under the 1998 and 2018 Data Protection Acts for sustained failures to comply with individuals' rights in subject access requests.
https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/06/blog-supporting-people-accessing-their-data-from-the-police/

d. Data loss[16], mass deletion process lack of security and audit safeguards.[17]
e. Data created or processed unlawfully through the use of emerging technologies.[18]
f. Children's rights are ignored in Prevent, described as a consensual programme. Personal data is not managed on the basis of consent and retention is excessive.[19]

3. National oversight and accountability

13. We are told that national oversight is not welcome or politically acceptable across policing. We suggest that it is not democratically acceptable for there to be the adoption of emerging technologies without it.

14. The government's proposals to reform the UK data protection regime were published on September 10, 2021. Data: A new direction proposes in Chapter 5.8 (para 409)[20] that:

> *"We must continue to review and simplify the regulatory landscape and the functions of the ICO to avoid duplication, overlaps and lack of clarity. For example, the* **oversight arrangements for the police's use of biometrics and overt surveillance are crowded and confusing.** *The Biometrics Commissioner covers police use of DNA samples, DNS profiles and fingerprints, and the Surveillance Camera Commissioner covers all use of surveillance cameras by specified public authorities (including local authorities and the police), while the ICO covers the processing of all personal data by the public and the private sector in the UK*."

15. Furthermore, in paragraph 410 it recommends consolidation under the ICO

> *"***The government will explore the potential for further simplifying the oversight framework by absorbing the functions of those commissioner roles into the ICO,*** which should bring benefits to data controllers and the public with a single route for advice, guidance and redress."*

16. This of itself might not be problematic as long as the necessary specialist knowledge and capability were brought with the roles and functions, and sufficient statutory weight were given to its enforcement and oversight within the other priorities of the ICO. However, such functions must be free from pressures of the duty to economic growth, made under paragraph 110(6) of the 2015 Deregulation Act[21]. In paragraph 321 the *Data: A new direction consultation* proposes instead to expand this duty.

> *"a new, statutory framework that sets out the strategic objectives and duties that the ICO must fulfil when exercising its functions. As* **the ICO's role becomes increasingly important for competition, innovation and economic growth,** *this strategic framework should empower the ICO to take greater account of impacts in these other domains as it supervises and enforces the UK's data protection regime."*

---

[16] In January 2021 the PNC experienced a data loss affecting 112,697 person records, recovered by 24 May 2021 .https://www.nao.org.uk/press-release/the-national-law-enforcement-data-programme/
[17] BBC (2021) Police probes compromised after computer records deleted https://www.bbc.co.uk/news/uk-55684320 The National Police Chiefs' Council said 213,000 records were deleted.
[18] BBC (2020) Facial recognition use by South Wales Police ruled unlawful https://www.bbc.co.uk/news/uk-wales-53734716
[19] The Guardian (2019) Family wins fight to delete child from Met anti-radicalisation records https://www.theguardian.com/uk-news/2019/dec/19/family-wins-fight-to-delete-child-from-met-prevent-anti-radicalisation-records
[20] 5.8 Biometrics Commissioner and Surveillance Camera Commissioner https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1016395/Data_Reform_Consultation_Document__Accessible_.pdf
[21] Statutory Guidance under paragraph 110(6) of the 2015 Deregulation Act https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/603743/growth-duty-statutory-guidance.pdf

17. The Information Commissioner regardless of whether it adopts the functions of *The Biometrics Commissioner* and the *Surveillance Camera Commissioner* should be exempted from the duty to economic growth as it may be in direct conflict with human rights. Balancing the public interest between these duties may be beyond the ken of a data regulator.

18. The Committee could consider recommending a new statutory regulator for police, technology, and criminal justice data ethics, into which the *Biometrics Commissioner* and the *Surveillance Camera Commissioner* would be adopted instead. This would provide the level of technology expertise to UK law enforcement agencies required for safe procurement processes with views to state security, and the applied use of emerging technologies. It would maintain registers of use by agencies and their contracted third parties, which were open to independent researchers for scrutiny, such as of machine learning algorithms. This would support demonstrable mechanisms to maintain public trust in emerging practices.

4. Deficit of democratic decision making: Live Facial Recognition

19. Following the brief consultation[22] (17 May—27 June 2021) to develop new Authorised Professional Practice (APP) on the use of Live Facial Recognition (LFR) defenddigitalme submitted a complaint to the College on the process due to its framing, content, short time period, and it being run in parallel to the Police, Crime, Sentencing and Courts Bill.

20. In a subsequent meeting in September with representatives of the Metropolitan Police, South Wales Police, the Home Office, and the College of Policing, senior officers confirmed their understanding that the use of Live Facial Recognition in UK law enforcement is a done deal. They expect no further parliamentary or public debate on whether LFR should be used, only the possibility for public engagement on how it will be used. The Metropolitan Police has adopted LFR for operational use. While senior officers recognise that the Bridges judgement[23] demands consistency of procurement standards or applied use, there are no mechanisms in place to deliver this.

21. The case made for using LFR and children is contradictory. The Bridges judgement stated, "children under the age of 18 will not normally feature in a watchlist due to "*the reduced accuracy of the system when considering immature faces*". Yet using LFR to identify missing children is one of the most common use cases in arguments we hear put forward.

22. We are told that a 'hybrid approach' to procurement will leave Chief Constables with the decision making on whether to procure Live Facial Recognition technology, and South Wales police is to be the 'Lead Force' offering advice on policy and procurement. The APP is expected to be published at the end of October 2021.

We are happy to answer any questions.

Defenddigitalme
September 2021

---

[22] College of Policing 2021 consultation *Police use of live facial recognition technolog*y
https://www.college.police.uk/article/police-use-live-facial-recognition-technology-have-your-say
[23] Liberty (2021) The Court held that there were "fundamental deficiencies" in the legal framework and that Ed Bridges' rights were breached as a result. [2020] EWCA Civ 1058
https://www.libertyhumanrights.org.uk/issue/legal-challenge-ed-bridges-v-south-wales-police/