Response to Call for Evidence

House of Lords Justice and Home Affairs Committee

New Technologies and the Application of the Law

Submitted by
Professor Lilian Edwards (Newcastle University)
Professor Derek McAuley (University of Nottingham)
Dr Lachlan Urquhart (University of Edinburgh)
and Dr Jiahong Chen (University of Sheffield)

5 September 2021

Introduction

1. Professor Lilian Edwards is Professor of Law, Innovation & Society at Newcastle Law School, and a member of the Alan Turing Institute; From September 2021 she is seconded to the Ada Lovelace Institute to lead their work on the EU AI Regulation. Professor Derek McAuley is Director of Horizon Digital Economy Research Institute, a Research Hub within the UKRI Digital Economy programme, and Deputy Director of the UKRI Trustworthy Autonomous Systems Hub. Dr Lachlan Urquhart is Lecturer in Technology Law at Edinburgh Law School, and Co-Investigator of the UKRI Trustworthy Autonomous Systems Node in Governance and Regulation. Dr Jiahong Chen is Lecturer in Law at Sheffield Law School, and has recently published a book on data protection regulation.

2. This submission aims to address a selection of questions formulated in the Committee's Call for Evidence by presenting findings and views based primarily on research undertaken by us although we have also drawn on publicly available sources. We will focus on certain case studies and areas of technology governance with a view to informing the Committee's inquiry. We would be happy to be contacted for further evidence and for this submission to be published in full.

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

3. **One key area of research in this field, and thus our main example in responding to this consultation, relates to live automated facial recognition technology ("AFR")**[1] which is increasingly used in the UK despite considerable controversy. The Metropolitan Police Services (MPS), for example, trialled the implementation of AFR at Notting Hill Carnival in 2017.[2] South Wales Police (SWP) also piloted the deployment of AFR between May 2017 and April 2019 in about 50 large public events, which was later found unlawful by the Court of Appeal in 2020.[3] Both police forces claimed that the purpose of using AFR in public spaces was to identify and locate the individuals on a

[1] Lachlan Urquhart and Diana Miranda, "Policing Faces: The Present and Future of Intelligent Facial Surveillance". https://doi.org/10.31235/osf.io/73wrh
[2] https://www.theguardian.com/uk-news/2017/aug/05/met-police-facial-recognition-software-notting-hill-carnival
[3] https://www.bbc.co.uk/news/uk-wales-53734716

"watchlist". Outside the UK, similar uses have been made by, e.g. police in the US[4] and China[5]. We will provide further evidence regarding the legality and regulation of AFR in our responses to questions below.

Question 2. What should new technologies used for the application of the law aim to achieve? In what instances is it acceptable for them to be used? Do these technologies work for their intended purposes, and are these purposes sufficiently understood?

4. New technologies used for law enforcement must not only protect the public and individuals, but also maintain – if not promote – the level of human rights protection. The introduction of new technologies is often justified on the basis that they increase efficiency by lowering costs. One example of this is the MPS's rollout of mobile fingerprinting devices. **In the public sector, however, cost-efficiency should not come as the sole consideration for law enforcement authorities when making decisions on the use of technologies.** It can serve as an additional justification, but only provided that the technologies prove to be effective in improving public safety and do not negatively impact on the rights and freedoms of the individuals involved.

5. The efficiency-focused mindset is also often evident in how new technologies are proposed to correct existing flaws in the criminal justice system. In the government's end-to-end rape review report earlier this year, for example, the technological response to the criticised "digital strip search" practice[6] has a clear emphasis on speeding up the digital forensics process.[7] While the report also mentions the need to develop selective data extraction methods, this should have been the main focus with a view to protecting the victim's rights and freedoms, including their privacy, access to justice and non-discrimination.

6. In this regard, conducting a comprehensive human rights impact assessment (HRIA) before the deployment of new technologies for law enforcement purposes is of great importance, which we will further elaborate below.

Question 3. Do new technologies used in the application of the law produce reliable outputs, and consistently so? How far do those who interact with these technologies (such as police officers, members of the judiciary, lawyers, and members of the public) understand how they work and how they should be used?

7. There is evidence-backed concern about the error rate of AI in the law enforcement context. Reports have emerged about the Home Office funding research projects to use AI to predict violent crimes, only to turn out to have a low level of accuracy.[8] **There is thus an urgent need to ensure law enforcement authorities carry out randomised controlled trials within the proposed deployment context to compare the performance of new technologies against existing practices before introduction to service.** Importantly, the trials and actual deployment should take into account the

[4] https://www.bbc.co.uk/news/technology-48339142
[5] https://www.washingtonpost.com/world/facial-recognition-china-tech-data/2021/07/30/404c2e96-f049-11eb-81b2-9b7061a582d8_story.html
[6] https://www.theguardian.com/law/2019/jul/23/police-demands-for-access-to-victims-phones-unlawful
[7] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1001417/end-to-end-rape-review-report-with-correction-slip.pdf, paras 93-101
[8] https://www.wired.co.uk/article/police-violence-prediction-ndas

contextual factors specific to the operation and situate the technologies in the authority's working practices. The SWP case, for example, has exposed the inadequacies of watchlist curation, highlighting the need for stricter operational oversight of decisions that can be subsequently audited, queried and accounted for.

8. **As regards the perceptions of those using these new technologies, our recent empirical research on AFR shows there is a high degree of scepticism and disbelief in AFR among frontline police officers.**[9] They express concerns about the effectiveness, accuracy and usefulness of the technology, acknowledging the need for a strong justification for deployment, or else undermining public confidence in police work.[10] Distrust in new technologies in law enforcement, whether within or outside the police force, could offset the advantages that the technologies may prove to have. We therefore call for a more participatory approach in decision-making regarding introducing new technologies by consulting frontline officers, the general public, civil society groups and other relevant stakeholders. This should also apply to scenarios where the technology is procured from the private sector, in which case stakeholders should be involved at the stage of design.

Question 4. How do technologies impact upon the rule of law and trust in the rule of law and its application? Your answer could refer, for example, to issues of equality. How could any negative impacts be mitigated?

9. The adoption of new technologies in law enforcement contexts often lacks robust tests on the quality of outputs prior to deployment. Hype, public relations and attempts to do more with less in terms of resources may drive uptake rather than clear evidence that the new technology improves results and does not have countervailing problems such as introducing errors, automation bias, non-transparency as to how it reached its conclusions, and incursions into privacy. One of the major grounds on which SWP's AFR deployment was ruled illegal by the Court was the force's failure to demonstrate the system does not exhibit unacceptable racial and sexual biases, and as a result, the failure to fulfil its public sector equality duty under the Equality Act 2010.[11] This shows how claims that new technologies can make policing "smarter" can sometimes be highly challengeable, if not entirely unfounded.

Question 5. With regards to the use of these technologies, what costs could arise? Do the benefits outweigh these costs? Are safeguards needed to ensure that technologies cannot be used to serve purposes incompatible with a democratic society?

10. There is a considerable debate currently about whether regulatory safeguards will unduly increase the costs of development and deployment of AI systems (in general, not just in law enforcement) in the EU. This debate has been spurred by the proposal of the draft framework for regulation in the EU AI Act.[12] Safeguards such as requiring high quality training data, and ensuring transparency and human oversight, have received criticism from some parts of industry. However, first, it is neither legal nor ethical to argue that technologies should be implemented if they pose serious risks to

[9] Lachlan Urquhart and Diana Miranda, "Policing Faces: The Present and Future of Intelligent Facial Surveillance". https://doi.org/10.31235/osf.io/73wrh
[10] Ibid.
[11] https://www.judiciary.uk/wp-content/uploads/2020/08/R-Bridges-v-CC-South-Wales-ors-Judgment.pdf, paras 163-202
[12] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206

human rights and equality, only simply to save money. Secondly, the AI Act and its impact assessment show that the costs can be manageable especially in a risk-based model of regulation. Haataja and Bryson have produced some helpful early work rebutting some of the more outlandish claims of extreme costs from lobbyists[13].

11. By contrast, there is also often a hype cycle that AI will be a magic bullet providing better services for less money, especially in the delivery of public services. History shows this is rarely true at least for delivery of a comparable service to the human-managed predecessor. **We recommend robust economic impact assessments before new largescale law enforcement AI is deployed and/or procured**; **AI systems should neither be assumed to be money-savers or money-wasters.**

Question 6. What mechanisms should be introduced to monitor the deployment of new technologies? How can their performance be evaluated prior to deployment and while in use? Who should be accountable for the use of new technologies, and what accountability arrangements should be in place? What governance and oversight mechanisms should be in place?

12. **Comprehensive human rights impact assessments (HRIAs) of new law enforcement technologies must be carried out**. The impact assessment process should address the relevant specific areas of concerns, and include a data protection impact assessment (DPIA) if personal data is involved,[14] and an equality impact assessment (EIA) if equality implications may arise.[15] For law enforcement authorities, the failure to carry out such assessments may render the deployment of a new technology unlawful under human rights, data protection or equality laws.

13. These assessments should be published and consultation should be enabled in a real and transparent sense with both the public and civil society prior to deployment. For much of the COVID emergency there has been an unwillingness by central government to publish impact assessments and this has impacted both public trust and possible scrutiny. This secretive tendency needs to be pushed back as we move towards the end of the acute pandemic cycle.

14. To support effective evaluation of the results and impacts of new technologies, it is crucial that law enforcement authorities, as well as independent oversight bodies, have sufficient access to scientific and technical expertise. Advisory boards with external, independent experts from technological or interdisciplinary backgrounds can be a helpful addition to the existing governance structure.

Question 7. How far does the existing legal framework around new technologies used in the application of the law support their ethical and effective use, now and in the future? What (if any) new legislation is required? How appropriate are current legal frameworks?

15. In the domestic UK context of law enforcement, probably the main legal safeguard most often consulted is **data protection law, as found primarily now in the UK GDPR, alongside the equality and human rights frameworks**. Data protection is however facing multiple challenges right now, especially in the wake of Brexit: both around compliance and oversight, and around the limitations of the legislation itself. Challenges to the legality of public sector and law enforcement AI systems

[13] See Meeri Haataja and Joanna J. Bryson, "What costs should we expect from the EU's AI Act?". https://doi.org/10.31235/osf.io/8nzb4
[14] https://ico.org.uk/media/2619985/ico-opinion-the-use-of-lfr-in-public-places-20210618.pdf
[15] https://researchbriefings.files.parliament.uk/documents/SN06591/SN06591.pdf

can, as the SWP case shows, be brought under the common law of judicial review, or by complaint to the various regulators involved. Currently, multiple supervisory authorities are involved, including the Information Commissioner, the Investigatory Powers Commissioner, and the Biometrics and Surveillance Camera Commissioner. Cooperative efforts may be needed from these authorities to strengthen the enforcement of existing law.

16. We are (like many researchers) concerned about the current level of enforcement of data protection law, especially in relation to law enforcement technologies. As a key example, in 2019, the Information Commissioner's Office (ICO) launched an investigation into police use of facial recognition technology, and concluded that "[t]here is some evidence of processing good practice by both SWP and the MPS" and that "there is no basis for the ICO to consider regulatory action" in the light of the High Court's ruling that the SWP pilot was lawful.[16] After that ruling was overturned by the Court of Appeal, however, no further actions were taken by the ICO.[17] **We suggest that the enforcement record of the ICO in this area should be reviewed and questions should be asked by the Committee about whether its efficiency is impeded by lack of resources, political hesitancy and a need to consider societal priorities as well as individual complaints.**

17. Some other challenges arise from the current legal framework itself. For example, our research has shown that increasingly ubiquitous machine learning (ML)-based algorithmic systems commonly raise serious concerns in terms of transparency, fairness and equality.[18] Professor Edwards's recent work for the Legal Education Foundation on automated decision-making in the public sector highlights many issues needing "fixed" in relation to both data protection safeguards for algorithms and common law judicial review.[19] It is clear data protection alone is not currently adequate to provide legal safeguards for public sector and law enforcement AI. This will be all the more true if the UK GDPR is "watered down" as has been recently proposed in the TIGRR report[20] and in comments by the DCMS Secretary, Oliver Dowden.[21] In particular, statements that Article 22 GDPR (that regulates automated decision-making) should be scrapped are deeply unhelpful. Despite Article 22's flaws, as matters stand it represents one of the few safeguards citizens have against flawed decisions concerning crucial human rights by automated systems such as public space AFR.

18. We would draw the Committee's attention to the idea of a comprehensive regulatory framework for building better, fairer, more transparent and less error-prone AI systems, not just in the context of law enforcement. This is the explicit aim of the EU's proposed AI Act.[22] **While the UK is under no obligation to implement the AI Act, we recommend that its solutions be carefully scrutinised as it is likely to become, like the GDPR before it, a global model for regulation.** Professor Edwards has

---

[16] https://ico.org.uk/media/about-the-ico/documents/2616185/live-frt-law-enforcement-report-20191031.pdf

[17] https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/08/ico-statement-on-the-court-of-appeal-judgment/

[18] Lilian Edwards and Michael Veale, "Slave to the Algorithm? Why a 'Right to an Explanation' Is Probably Not the Remedy You Are Looking For". https://scholarship.law.duke.edu/dltr/vol16/iss1/2/

[19] See https://research.thelegaleducationfoundation.org/wp-content/uploads/2021/07/FINAL-Legal-and-Regulatory-Frameworks-Governing-the-use-of-Automated-Decision-Making-and-Assisted-Decision-Making-by-Public-Sector-Bodies-1.pdf; for context see https://www.thelegaleducationfoundation.org/articles/tlef-response-to-law-commission-consultation-calls-for-reform-to-the-law-governing-the-use-of-automated-and-assisted-decision-making-systems-by-public-bodies

[20] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/994125/FINAL_TIGRR_REPORT__1_.pdf, pp. 49-53.

[21] https://www.wired.co.uk/article/uk-change-gdpr-eu-adequacy

[22] For an analysis of the key parts of the proposed AI Act, see Michael Veale and Frederik Zuiderveen Borgesius, "Demystifying the Draft EU Artificial Intelligence Act". https://osf.io/preprints/socarxiv/38p5f

prepared a briefing on the AI Act for the Ada Lovelace Institute, which can be provided to the Committee for reference.

19. **The proposed AI Act is to deem certain biometric surveillance systems as "unacceptable risk" and thus as "red lines" to be banned. Real-time biometric identification systems (which covers AFR) would be prohibited in principle.[23] We believe clear restrictions should be placed on the use of law enforcement AFR but we also counsel that the AI Act proposal's "red lines" are insufficient and not a good model.**

20. There are notable problems with the EU implementation of a law enforcement biometric surveillance ban, which should be carefully reviewed. In effect, it actually covers a limited scope. Only *'real-time*' biometric identification systems are banned, i.e., those that identify individuals at a distance by comparing the biometrics of the observed subject with a biometric database without "significant delay".[24] Yet as the EDPB-EDPS joint opinion observes, post remote biometric ID, e.g., after a protest march, is as likely to have a chilling effect on free speech and assembly as real-time.[25] Also, "publicly accessible spaces" does not cover places that are private in nature and normally not freely accessible for third parties, including law enforcement authorities, such as homes, private clubs, offices, warehouses and factories. Online spaces are also not included in "publicly accessible spaces".[26] The restriction to law enforcement purposes excludes private security even though it may represent similar threats to fundamental rights. National security uses will also be excluded by virtue of the scope of EU law.

21. The exceptions listed are so wide that it is hard to believe one could not be invoked at any given time. In fact, it is likely the "ban" imposed by the proposed AI Act is less stringent than existing data protection law under the GDPR and the Law Enforcement Directive (LED). Perhaps most egregiously, by purporting to ban biometric AI but providing a shelf of get-outs, the proposal may give a false sense that "something has been done" while reassuring and normalising biometric surveillance practices, which in reality are more likely to fall into "high-risk".[27]

Question 9. Are there relevant examples of good practices and lessons learnt from other fields or jurisdictions which should be considered?

22. See our discussion above concerning the EU's proposed AI Act. The debates here around "unacceptable risk" and "high risk" AI systems, the latter including many law enforcement and criminal justice AI systems (e.g. sentencing, bail and "robo-justice" systems), will be extremely germane to the Committee's work. We also point to the planned work by the Law Commission in its next work programme on automated decision making in the public sector.

---

[23] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206

[24] Ibid, Article 3(37).

[25] https://edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-52021-proposal_en, para 31.

[26] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206 Recital 9

[27] Ibid, Annex III.

Question 10. This Committee aims to establish some guiding principles for the use of technologies in the application of the law. What principles would you recommend?

23. **We recommend the principles elaborated by the Legal Education Foundation on automated decision making (ADM) in the public sector**.[28] We feel they are as relevant to the more limited or adjacent domain of law enforcement and adjudication. These are:

- Safeguards should address both ADM and ASDM (Assisted Decision Making Systems – i.e. systems which cannot strictly be described as "solely automated") in legal frameworks, as very few systems are strictly wholly autonomous.
- Ensure that ADM/ASDM systems uphold existing privacy, equalities and human rights laws.
- Secure meaningful and effective transparency in relation to the use of ADM/ASDM systems e.g. by public registers (a solution also recommended by the EU's proposed AI Act). For citizens, secure legally enforceable rights to an explanation of how systems make decisions for them as individuals as well as generically.
- Deliver certainty for public bodies, suppliers and individuals around the circumstances in which ADM and ASDM systems can be used.
- Support meaningful public engagement in determining appropriate uses of ADM/ASDM.
- Focus governance at the *design and deployment* stage. Make sure that relevant rights e.g. transparency can be exercised against external vendors and that *procurement* is subject to scrutiny, given many or most public AI systems are not developed "in house".
- Guarantee independent *external scrutiny* to ensure the efficacy and accuracy of ADM/ASDM systems.
- Ensure clear lines of accountability for decisions taken by ADM/ASDM systems.
- Provide timely, appropriate, accessible and cost-effective routes to redress where this is required.

[28] https://research.thelegaleducationfoundation.org/wp-content/uploads/2021/07/FINAL-Legal-and-Regulatory-Frameworks-Governing-the-use-of-Automated-Decision-Making-and-Assisted-Decision-Making-by-Public-Sector-Bodies-1.pdf