Archie Drake & Perry Keller, King's College London — Written evidence (NTL0011)

Thank you for the opportunity to submit evidence to this Inquiry. We are making this submission on an individual basis, drawing on recent professional experience.

Our submission is based on a research investigation undertaken over the first half of 2021 in partnership with the British Institute of International and Comparative Law (BIICL). The research sought views on recent legal contestation of automated decision-making, including artificial intelligence, across various sectors, including criminal justice, from groups composed of civil society activists, legal practitioners and academics in the UK. A public panel event in February established a scope of work for full investigation through a 'policy lab' expert workshop in May involving 40 participants, co-chaired by a network of other researchers from across the UK. The workshop findings are under peer review, with the objective of publication before the end of 2021.

This work was funded by the Engineering & Physical Sciences Research Council under the Trust in Human-Machine Partnership (THuMP) project (EP/R033722/1).

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

1. Policymakers have tended to neglect legal actions as a source of evidence on the issues involved in automating decision-making processes. Examples identified in our investigation as relevant to application of the law in a criminal justice context included:

- *Hamilton and others v Post Office Ltd [2021] EWCA Crim 577* and others. Over 1999 – 2015, the Post Office reportedly used evidence based on its Horizon accounting and stocktaking software to prosecute 736 people successfully for theft and other criminal offences. 59 of these convictions have now been overturned, highlighting over-estimation of the dependability of computer-generated evidence.[1]
- *R Bridges v CC South Wales Police [2020] EWCA Civ 1058*. A member of the public challenged past use of automated facial recognition (AFR) software by the police in a pilot project. This was found to be unjustified interference with the European Convention on Human Rights (ECHR) Article 8 right to private life. Deficiencies were also found in the force's Data Protection Impact Assessment (DPIA) and compliance with the Public Sector Equality Duty (PSED).
- *S. and Marper v. The United Kingdom, 2008*. Two individuals applied to the European Court of Human Rights to argue that indefinite retention of

[1] Christie, J. (2020). The Post Office Horizon IT Scandal and the Presumption of the Dependability of Computer Evidence. Digital Evidence and Electronic Signature Law Review, 17, 49

DNA samples taken from them constituted an unjustified interference in their rights to private life under Art.8 ECHR. This case has, of course, been followed by many others concerning police records, such as *R (Catt and T) v Commissioner of Police of the Metropolis* [2015] UKSC 9 and *Catt v. the United Kingdom,* (Application no. 43514/15, 24 January 2019). While these cases focus on record scope and retention, law enforcement records provide essential and often highly sensitive data for new applications of data analytics.

- *West Midlands data ethics committee National Data Analytics Solution (NDAS) Most Serious Violence recommendation*. The West Midlands Police data ethics committee recommended that the NDAS 'Youth and Most Serious Violence' project should not proceed because of concerns about lack of statistical validity and it was withdrawn.[2]

2. It was also apparent from examples encountered during our investigation that there are serious concerns about uses of technology in the application of the law in the field of immigration. Notable legal actions included:

- *Ahsan v Secretary of State for the Home Department (Rev 1) [2017] EWCA Civ 2009* and others. The Home Office's reliance on technologically-determined suspicions about the validity of English language testing in immigration processing has caused massive confusion and probable injustice.[3]

- *Home Office streaming tool.* The Home Office has reportedly agreed to stop using a visa application streaming tool which involved racial discrimination, although it remains unclear how exactly the relevant algorithm works.[4]

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?

3. Those making decisions about any new technology used for the application of the law should ensure that the technology itself complies with applicable law. If the law is unclear in relation to a new technology, either in substance or from the perspective of specific decision-makers, then clarification should be sought before proceeding to use. The law may require or authorise certain legal obligations to be balanced with other legitimate objectives, but in no case is it acceptable for uses of technology to disregard

[2] Oswald, M. (2021). A Three-Pillar Approach to Achieving Trustworthy and Accountable Use of AI and Emerging Technology in Policing in England and Wales: Lessons From the West Midlands Model (SSRN Scholarly Paper ID 3812576). Social Science Research Network. https://doi.org/10.2139/ssrn.3812576

[3] National Audit Office. (2019). https://www.nao.org.uk/wp-content/uploads/2019/05/Investigation-into-the-response-to-cheating-in-English-language-tests.pdf

[4] The Joint Council for the Welfare of Immigrants. (2020). We won! Home Office to stop using racist visa algorithm. https://www.jcwi.org.uk/News/we-won-home-office-to-stop-using-racist-visa-algorithm

potentially applicable law or to consider lack of legal clarity as an appropriate context in which to proceed.

4. With the passage of time, understandings of the various purposes intended for relevant technologies and of the often-unintended ways in which they fail to meet legal standards have improved. Four related bodies of law are now considered most relevant:

- *Human rights*. There has been a disregard for basic rule of law requirements or an unnecessary or disproportionate interference with peoples' private and family lives, homes or communications (e.g. *Bridges*).
- *Data protection*. A point of special concern is that DPIAs are not being produced in accordance with the law or to any reasonable standard of quality or consistency.[5]
- *Discrimination*. Authorities have struggled to implement new technologies in ways that comply with the Equality Act 2010 including the PSED.[6]
- *Public administration*. In particular: duties in respect of procedural fairness, the duty of candour, other rights in respect of judicial review and freedom of information requests.[7]

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?

5. Our investigation suggested that the biggest problem in terms of reliability is poor quality in technology products and services used by public bodies, rather than issues inherent to the technologies themselves. Third party vendors are over-claiming system capabilities for commercial advantage and failing to flag the need to invest sufficiently in high-quality systems or data management. It is all too rare that authorities decline to adopt technology because of quality concerns, as in the West Midlands NDAS example given above. More often the issues seem to be emerging later in the form of large-scale injustices, as in the Post Office and Home Office English language examples.

[5] For example, in the government's recent applications of technology to monitor behaviour relating to Covid-19 rules: Veale, M. (2020). Analysis of the NHSX Contact Tracing App 'Isle of Wight' Data Protection Impact Assessment. LawArXiv. https://doi.org/10.31228/osf.io/6fvgh; Joint Committee on Human Rights. (2020). The Government's response to COVID-19: Human rights implications. https://publications.parliament.uk/pa/jt5801/jtselect/jtrights/265/26509.htm

[6] See for example Allen, R., & Masters, D. (2019). In the Matter of Automated Data Processing in Government Decision Making: Joint Opinion. https://www.cloisters.com/wp-content/uploads/2019/10/Open-opinion-pdf-version-1.pdf

[7] See for example the cases discussed in Maxwell, J., & Tomlinson, J. (2020). Public law principles and secrecy in the algorithmic state. https://www.lag.org.uk/article/207441/public-law-principles-and-secrecy-in-the-algorithmic-state

6. The question of how far people understand these technologies when interacting with them is very difficult to answer, not least because of significant variation in the people and in interactions. Our investigation suggested that judges' application of the law to facts involving technology is perceived to be uneven, for example, especially in the lower courts as they interpret principles established at superior levels.[8] It also suggested that the public have become increasingly familiar with rogue algorithms and other 'computer says no' frustrations, but that there is very little systematic governance attention to these burdens on the public or related complaints or disputes.

7. But there are also indications that understandings relevant to public policy are beginning to advance as time passes. Our investigation suggested three insights in particular:

- Very often, members of the public are simply not aware that relevant technologies are being deployed or that they can exercise their rights to obtain further information.
- The problem of understanding is relevant earlier and at a greater distance from 'technology' than most people realise, especially senior administrative managers' and ultimately ministers' originating decisions about whether and how technology will be deployed.
- Lawyers generally and members of the judiciary especially have a limited but rapidly growing understanding of relevant technologies.[9]

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?

8. A vicious cycle of trust is now apparent in legal contestation of relevant technologies in the UK. A proliferation of legal actions and a growing community of committed professionals and advocacy organisations are exposing weaknesses in government technology policy implementation, driving processes for building confidence and trust in technology in an unintended direction. This exacerbates the low level and negative trend in public trust for relevant technology.[10]

9. The question of impacts on the rule of law and on trust in the rule of law are more difficult to answer. On the one hand, it may be that growing legal contestation tends to demonstrate the relevance of law to technological change and its effectiveness as a principles-based constraint on power. On the other, policy may tend to undercut any such institutional development if government

[8] Participants in our investigation referred in particular to the way in which principles established in *Bridges* were interpreted in cases such as The Motherhood Plan v HMT & HMRC [2021] EWHC 309 (Admin) and The 3million Ltd, R (On the Application Of) v Secretary of State for the Home Department [2021] EWHC 1159 (Admin)

[9] See for example The Law Society. (2019). Algorithm use in the criminal justice system report. https://www.lawsociety.org.uk/support-services/research-trends/algorithm-use-in-the-criminal-justice-system-report/

[10] Edelman. (2021). Trust Barometer Tech Sector Report. https://www.edelman.com/sites/g/files/aatuss191/files/2021-03/2021%20Edelman%20Trust%20Barometer%20Tech%20Sector%20Report_0.pdf

continues to authorise, tacitly or carelessly as well as explicitly or deliberately, technology implementations that are poor quality, disregard the law, exploit legal uncertainty and/or evade public disclosure altogether.

10. Unhelpfully from a trust perspective, government has used legal actions to refine authorisations for uses of technology (for example on AFR, the Surveillance Camera Commissioner quickly responded to *Bridges* by issuing guidance explicitly aimed at supporting its use by forces).

11. The government's own AI Council advisory group has observed that the government's strategic direction on AI is 'plagued by public scepticism and lack [of] widespread legitimacy' in ways that suggest a 'fundamental mismatch between the logic of the market and the logic of the law'.[11]

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?

12. Our investigation suggested that the risk of harm derives mainly from operator misuse, confusion or incompetence rather than inherent qualities of technology. The main sources of risk of harm are as follows:

- Intellectual property (IP). Public authorities looking to implement ADM systems are often not entitled to know much about the systems they are using because of suppliers' 'aggressive' commercial confidentiality standards and associated practices.[12]
- Lack of clear responsibility. There are issues with 'the extent to which discretionary agency is delegated to technology, despite awareness of potential technological limitations'.[13]
- Harm diffusion. Relevant technologies often affect large numbers of people in compounding ways that are subtle or intangible and only infrequently develop into clear detriment.

13. It is certainly possible that these harms, if allowed to develop unchecked, may prove incompatible with democratic society. Two safeguards are needed to mitigate this risk:

- **More time to develop higher-quality institutional supports for technology implementation in the application of the law carefully, to build legitimacy**, including: steps to clarify which organisations take responsibility for which aspects of implementation and operation

[11] AI Council. (2021). AI Roadmap. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/949539/AI_Council_AI_Roadmap.pdf

[12] As is widely noted, this issue has been a focus of attention for relevant debates in the United States. See for example Liu, H.-W., Lin, C.-F., & Chen, Y.-J. (2019). Beyond State v. Loomis: Artificial Intelligence, Government Algorithmization, and Accountability. International Journal of Law and Information Technology, 27. https://doi.org/10.1093/ijlit/eaz001

[13] Fussey, P., Davies, B., & Innes, M. (2021). 'Assisted' facial recognition and the reinvention of suspicion and discretion in digital policing. The British Journal of Criminology, 61(2), 325–344. https://doi.org/10.1093/bjc/azaa068

(including unanticipated harms); development of mechanisms for oversight at earlier stages of decision-making processes and for improved procurement systems and standards (including on IP); development of credible levels of public awareness about what is being done; and public debate about the nature of diffuse harms and sufficiency of legal recourse.

- **Clear governmental affirmation of the rule of law.** There are obviously limits as to the legality of relevant technology implementation. More should be done by authorities to issue clear signals that some applications are illegal. In this regard, the question should be not just how to regulate a particular technology appropriately, but whether the technology should be used at all (e.g. biometric surveillance in public spaces).

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?

14. The first and most important mechanism which should be introduced to monitor the deployment of new technologies is broader public awareness. The Committee for Standards in Public Life has observed that 'the government is failing on openness' and the 'lack of transparency is particularly pressing in policing and criminal justice'.[14] At a minimum, relevant authorities should be obliged to disclose which new technologies are in use (for example using an annual procurement information return compiled and published by a central authority, or by obliging prior publication of and consultation on DPIAs).

15. Performance evaluation and advisory oversight functions should be independent from implementing organisations as in the 'West Midlands' example, with particular attention to the mobilisation of technological expertise and robust ethical standards (including diverse representation from local communities as well as legal inputs to support compliance). In particular the protection of commercial confidentiality and trade secrets in the use of new technologies by public authorities needs robust, independent mechanisms of evaluation and oversight to ensure that resort to this legitimate ground for confidentiality is not abused.

16. Accountability arrangements need to start at ministerial levels and extend to the general policy environment established for relevant sections of the criminal justice system. These problems start with ministers and the policy 'signals' they send. The Secretary of State for the Home Department, the Lord Chancellor and Secretary of State for Justice and the Minister for Crime and Policing should be called upon to articulate how the government's vision of technological change in the system safeguards its effectiveness and legitimacy.

[14] The Committee on Standards in Public Life. (2020). Artificial Intelligence and Public Standards: Report. https://www.gov.uk/government/publications/artificial-intelligence-and-public-standards-report

17. There are three essential governance mechanisms that should be in place:

- **Improved channels for public participation through the law.** Given the significance of the issues, it is not enough for the government to limit public engagement to consultations and limited focus group-type "citizens' juries". The Law Commission should be asked to review and reinforce relevant existing public information rights and systems (including judicial review, freedom of information, subject access requests and litigation disclosure rules) to ensure they are adequate for the needs of a 'datified' and digitised society.
- **Audit processes.** Relevant public bodies should be required to keep full and systematic records of all data processed by technological systems, using specified provenance standards and to be retained for periods comparable to financial information. Relevant agencies including the National Audit Office (NAO) and the Information Commissioner's Office (ICO) should be properly funded and empowered to carry out relevant investigations proactively.
- **Regulatory coordination.** The criminal justice system lacks a coordinated regulatory approach. It has become clear that CDEI does not have the mandate or resourcing to address the issues involved effectively. Steps should be taken to ensure regulatory coordination over technology uses in the criminal justice system. A good step would be to task the Criminal Justice Board to initiate a sub-group to make recommendations on process and resourcing.

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?

18. The main problem is compliance with the existing legal framework, not the framework itself. Many of the participants in our investigation considered that government policy is irresponsible in that it has not sought genuine engagement with the issues. Criminal justice organisations, and police forces especially, have a reputation in the field for uncritical technology implementation encouraged by permissive central policy. Regulators are chronically under-resourced and are effectively deciding not to enforce relevant law where there are political sensitivities. Rather than encouraging innovation, legal uncertainty tends to harm business and innovation as well as public trust in the criminal justice system (and technology).

19. Two specific new pieces of legislation might be appropriate. First, it would be appropriate to legislate to ban clearly harmful or high-risk applications of technology (such as AFR) where these are not accompanied by robust arrangements to improve public accountability.[15] Second, it would be appropriate to introduce a measure firmly aimed at

[15] Williams, R. (2019). Accountability key to the adoption of surveillance technology. Oxford Law Faculty. https://www.law.ox.ac.uk/centres-institutes/centre-criminology/blog/2019/05/accountability-key-adoption-surveillance

establishing improved arrangements for transparency and public participation in setting standards for relevant uses of technology (eg the 'Public Interest Data Bill' proposal mentioned above).

Question 8. How can transparency be ensured when it comes to the use of these technologies…?

20. As part of broader research project work focused on fostering trust in human-machine interactions[16], our investigation highlighted how useful it is for transparency and other legally-relevant standards to form an integral part of the technology design process to ensure that these standards have a meaningful presence in subsequent applications.

21. Pro-actively providing very clear, basic information about the *existence* of relevant technology systems is the best starting point for transparency. This accords with a recent survey for CDEI stressing the need for 'active, up-front communication that the algorithm is in use, to those affected'.[17]

2 September 2021

[16] See for example Canal, G. et al. (2020). Building Trust in Human-Machine Partnerships. Computer Law & Security Review, 39, 105489. https://doi.org/10.1016/j.clsr.2020.105489
[17] BritainThinks. (2021). Complete transparency, complete simplicity. https://www.gov.uk/government/publications/cdei-publishes-commissioned-research-on-algorithmic-transparency-in-the-public-sector/britainthinks-complete-transparency-complete-simplicity