Professor Charles Raab, Professorial Fellow, School of Social and Political Science, University of Edinburgh Fellow, The Alan Turing Institute — Written evidence (NTL0014)

Introduction: Writing in my personal capacity, I wish to supplement the Oral Evidence I gave to the Committee on 22 June 2021, by considering a few of the Committee's questions but without addressing each in turn. For reference, these are QQ 10, 8, 6, 5 in order of emphasis.

1. The police community in this country is rightly proud of the Peelian Principles of 1829, but these need to be augmented and adapted to address the issues raised by the use of today's – and tomorrow's – technologies in preventing and detecting crime, maintaining public order, and in other activities in the law enforcement system. These issues arise from the use of novel technological innovations, including their use in the processing of data, that require new thinking and ethical debate as well as reconsideration of the regulatory environment of laws and other policy instruments that purport to oversee and govern them. But the questions posed by these developments have a longer lineage in the fundamental theory and practice of the relationship between people and the state in terms of the rule of law, and some of them have been visited before, and in more general terms, by previous inquiries.[1]

2. Artificial Intelligence (AI) is prominent in these technologies and is used in many data-based analytical applications within law enforcement. There is no single definition of AI, but as the European Commission puts it, AI "refers to systems that display intelligent behaviour by analysing their environment and taking actions – with some degree of autonomy – to achieve specific goals. AI-based systems can be purely software-based, acting in the virtual world (e.g. voice assistants, image analysis software, search engines, speech and face recognition systems) or AI can be embedded in hardware devices (e.g. advanced robots, autonomous cars, drones or Internet of Things applications)."[2]

3. The Committee's aim to establish some guiding principles for the use of these technologies in the application of the law is welcome. However, it is unlikely that such principles will vary substantially from those that feature in the dozens of generally applicable ethics frameworks that have been proposed by organisations and individuals around the world in the last few years.[3] This is an advantage, because the Committee can borrow rather than re-invent. It can

[1] See, for example, House of Lords, Select Committee on the Constitution, 2nd Report of Session 2008-09, *Surveillance: Citizens and the State*, Volume I: Report, HL Paper 18-I.
[2] Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions on Artificial Intelligence for Europe, Brussels, 25.4.2018COM (2018) 237 final.

[3] In 2019, some 80 ethical frameworks for automated decision-making systems were identified, emanating from governments, international agencies, companies, non-governmental bodies, academic institutions and others around the world; see AlgorithmWatch (2019) *AI Ethics Global Inventory*, https://algorithmwatch.org/en/project/ai-ethics-guidelines-global-inventory/; accessed 02/09/21

encourage those concerned specifically with the application of the law to measure their performance against ethical standards that are becoming well recognised, and to which the public may increasingly expect law enforcement to adhere.

4. There is no tidy inventory of ethical principles having the identical label across the welter of frameworks and lists, although there are some close resemblances. Among the most common are privacy protection, accountability, fairness, non-discrimination, justice, transparency, safety and cybersecurity, serving the common good, explainability, and human oversight.[4] Further themes are also available for evaluating actual performance. They include a mixture of abstract and more concrete procedural norms, including robustness and resilience, human wellbeing, quality assurance, auditability, enforcing sanctions, ensuring human rights, and complementing humans.[5] It is a matter for consideration whether one word better expresses the essence of a principle than another; and how many principles are required. Keeping it simple and as non-technology-specific as possible is probably the best course, if headline principles are required in the first instance.

5. How ethical principles relate to legal prescription is a further important question: as reaching parts that law cannot easily reach? As expressing the ethical bottom line of the legal rule? As more comprehensible by laypersons? Sceptics may see an emphasis on adherence to ethics-related principles as a soft option in comparison with legal compliance and sanctions, especially when ethics form part of an organisation's self-regulatory approach to protecting the public's rights or interests. 'Virtue signaling' or 'ethics washing', and the use of ethics mainly as a public-relations strategy for covering organisational backs, justifiably attracts adverse comment. This is partly because some ethical precepts are highly abstract, verging on mantras and mottoes. The OECD's five ethics-related principles for 'responsible stewardship of trustworthy AI' remain largely at that level.[6]

6. Focusing upon the development of AI rather than its use in specific domains, the European Commission High-Level Expert Group on Artificial Intelligence's prominent *Ethics Guidelines for Trustworthy AI* drew upon myriad ethics frameworks to identify four principles (alternatively seen as 'rights' and 'values'): respect for human autonomy, prevention of harm, fairness, and explicability. [7] But inventories of high-level principles court irrelevance in the

---

[4] Hagendorff, T. (2019) 'The Ethics of AI Ethics: An Evaluation of Guidelines', https://arxiv.org/pdf/1903.03425.pdf; accessed 02/09/21

[5] Clarke, R. (2019) 'The OECD's AI Guidelines of 22 May 2019: Evaluation against a Consolidated Set of 50 Principles', http://www.rogerclarke.com/EC/AI-OECD-Eval.html; accessed 02/09/21

[6] OECD (Organisation for Economic Co-operation and Development) (2019) *OECD Principles on Artificial Intelligence*, https://www.oecd.org/going-digital/ai/principles/; accessed 02/09/21

[7] European Commission High-Level Expert Group on Artificial Intelligence (2019) *Ethics guidelines for trustworthy AI*; A few months earlier, they had identified five: beneficence, non-maleficence, autonomy, justice and explicability. This change attests to the fluidity of such identification and its susceptibility to the vagaries of committee work.

law-enforcement field if less attention is paid to how they may be implemented in practice. More detailed work is needed on how to apply principles to the specific technologies that are used in specific law enforcement operations, and this can be ambiguous.

7. The EC's Expert Group has tried to dive more deeply into subsidiary issues and questions in putting principles to work, but became entangled in weeds.[8] However, if their, or other, principles can be appropriately transposed into procedures, guidelines, training, reflection and support that can be used 'on the ground' – both in technological development and in ultimate deployment – they could be useful in addressing not only the intended purposes to which technologies are applied, but in thinking about unanticipated and undesirable effects as well, their likelihood, and possible mitigations. Applying ethics is thus a question of augmenting the application of existing legal requirements for, for example, accountability and transparency, by means of other instruments. These could include codes of practice that can be adaptable to rapidly changing technologies and operational circumstances, provided they show how abstract principles may have traction in specific law-enforcement and public-order contexts and operational settings such as public spaces, or in predicting the location or the perpetrators of crime.

8. In addition, the application of principles to the specifications and procurement processes for equipment and analytical resources that are used in these law enforcement operations should not be neglected, given the lucrative market's persuasive promotion of technology- or data-driven systems, and the public policy or operational push to become equipped with high-tech law enforcement instruments. In practice, the collaborative relationship between law enforcement and the private sector in the use of, for instance, live facial recognition (LFR) systems, is growing, opaque, and insufficiently regulated by legal or ethical means.[9]
9. Moving from principles to practice would involve the assistance of organisations in and outwith the structures of law enforcement to develop the more detailed guidance, educational materials, and deliberative activity

---

[8] The bottomless pool includes 7 requirements, 23 themes, 60 questions, and 69 sub-questions to be addressed in developing and assessing trustworthy AI.

[9] Live facial recognition (LFR) is perhaps the most prominent and controversial among recent uses of technology in law enforcement, and has been the subject of litigation as well as critical, regulatory and parliamentary response; see Scott, E. 'Facial recognition technology: police powers and the protection of privacy', House of Lords Library, 31 March 2021: https://lordslibrary.parliament.uk/facial-recognition-technology-police-powers-and-the-protection-of-privacy/, accessed 02/09/21, and the many useful sources linked to this. The Biometrics and Forensics Ethics Group (BFEG) examined a number of causes for concern about public (police)-private collaboration in LFR, including data use and sharing, algorithms and machine learning, discrimination and bias, links with other biometric modalities, the construction and use of watchlists, the effect of the use of LFR to police private spaces used by the public, and deficiencies in governance and independent oversight. These, and BFEG's 7 recommendations, can be found in *Briefing note on the ethical issues arising from public-private collaboration in the use of live facial recognition technology (accessible)*, 21 January 2021, https://www.gov.uk/government/publications/public-private-use-of-live-facial-recognition-technology-ethical-issues/briefing-note-on-the-ethical-issues-arising-from-public-private-collaboration-in-the-use-of-live-facial-recognition-technology-accessible, accessed 02/09/21.

necessary to move closer to the level at which the everyday application of the law takes place, and at which ethical processes are most needed. Law enforcement-related think-tanks, institutes, ethics committees and panels, advocacy and civil-society groups, academic research bodies, and the like have begun to flourish in this country and make important contributions to debates over the use and misuse of technologies. Their practical knowledge, skills and perceptions in and around the application of ethics are important resources for the implementation of any relevant principles that the Committee identifies. In particular, the appearance and reality of the independence of these organisations from Government and from law enforcement itself are indispensible assets for the credibility and public acceptance of their outputs, and should be safeguarded.

10. It would be helpful, therefore, if the Committee gave a steer towards understanding better what principles mean in practice and how they can be embedded to foster a culture of ethical discourse and conduct, meshing with law-enforcement governance structures for oversight and accountability that can monitor the leveraging of principles into practice. This involves knowledge of technologies, their capabilities and limitations, and the decision-making contexts in which they are actually used. It also requires taking on board the experiences and perceptions of persons who are the recipients of policing and other parts of the system of law-enforcement and justice, and whose rights are potentially affected. What, for example does 'fairness' mean in the use of drones, body-worn cameras, crime prediction, and automatic number-plate recognition? What 'harms' may be caused – and to whom – by the surveillance and data-gathering operations in which these technologies are used? What would a change in the design or method of deployment of a camera, a sensor, or an algorithm mean in terms of exacerbating or ameliorating infringement of the freedom of assembly, privacy, and other rights enjoyed in a democratic society? How serious is the 'chilling effect' or the racial and other discrimination that is considered to result from technology-assisted surveillance, and what are its consequences for the way people go about their lawful activities? How might the circumstances of using a device – for example, turning a camera on or off, changing its angle of vision, or networking it to other devices – change the relationship between the police and the public, erode or enhance trust, and exacerbate or mitigate a harm?

11. Questions like these bring principle and practice together, often in some tension. Guidance should be developed for reconciling them, and for engaging in the deliberation that could lead to ethically justifiable applications of technology to their prohibition, or to a moratorium. Guidance as well as transparency are also required in applying the legal and ethical principles of necessity and proportionality in the use of AI and other technologies, and of explaining the reasoning behind conclusions about this in each case. These decisions are often obscure, leaving it up to the organisation – an interested party with a worthy mission and ethos of promoting 'safety'– to decide the 'balance' of benefits and harms without sufficiently explaining how this was arrived at.

12. An appropriate place for addressing many questions is in the impact assessments that may be required for new applications of technology and systems.[10] These assessments focus upon explanations of how a system works,

what the provenance and flow of its data are, what the potential benefits and harms might be, how harms would be mitigated, and other questions aimed at elucidating operational, legal, and ethical dimensions. In the best case, impact assessment requires descriptive answers, not box-ticking, and is performed at the beginning of a proposed adoption of a new technology or system so that it can play a part in the formation of the latter and in deployment. However, if the impact assessment is carried out under the rubric of privacy or data protection alone, it may miss crucial ethical dimensions. Enhanced versions of impact assessment inquire into human rights, ethical, and societal implications (e.g., for vulnerable communities) that go beyond the impact on individuals as such and their legal rights to privacy and data protection. [11] The obligation to undertake any of these versions could involve legislation. Especially if the assessment is published, it can be an important instrument in strengthening adherence to ethical principles, in gaining or retaining public confidence, and in demonstrating trustworthiness in ways that are more convincing than slogans and pledges, or compliance with legal requirements.

13. The Biometrics and Surveillance Camera Commissioner (and previously the separate Commissioners), the Scottish Biometrics Commissioner, and the Information Commissioner have important and complementary parts to play in guiding, overseeing, regulating, and advising on the use of AI and other technologies in law enforcement from standpoints that are independent from Governments. Their ability to tap into networks of expertise, both domestically and globally, is an asset. Commissioners' roles need strong support, and expansion of scope, in the face of the growing impetus towards high-tech law enforcement and its potential implications for individuals and society, whether benign or adverse. It would be a matter for concern if these bodies' influence and – where available – exercise of powers in the service of responsible innovation and use, and in the public interest, were to be curtailed by changes in the regulatory landscape aimed at accommodating technological development.

3 September 2021

---

[10] For law enforcement DPIA, see DPA 2018, Part 3, sec. 64.

[11] Types of impact assessment are discussed in Raab, C. (2020) 'Information Privacy, Impact Assessment, and the Place of Ethics' and sources cited therein. 'Algorithmic impact statements' are proposed by Selbst, A. (2018) 'Disparate Impact in Big Data Policing', *Georgia Law Review* 52: 109-195