Dr Matthias Wienroth (Vice-Chancellor's Senior Fellow in Criminology/Sociology) Dr Carole McCartney (Professor of Law and Criminal Justice) Dr Delphine Defossez (Lecturer in Law), Ms Angela Paul (PhD candidate in Law), and Dr Liam Ralph (Lecturer in Criminology and Policing) at the Centre for Crime and Policing & the Science and Justice Research Interest Group, Northumbria University— Written evidence — Written evidence (NTL0022)

1. Introduction

1.1. We are a group of researchers affiliated with the Centre for Crime and Policing and with the Science & Justice Research Interest Group at Northumbria University. Opinions expressed in this document do not represent an institutional position. We welcome the opportunity to offer insights on ethical, legal, practical and sociotechnical aspects of emerging technological developments in policing and submit our expertise in support of the work of the Committee. Included are general comments on key issues, with some focussed views on individual case studies. We have not attempted to answer each consultation question in turn, but provide an overview that nonetheless address many questions posed. To answer fully each of the questions would result in a much lengthier document. As the issues are many and some are complex, they are set out succinctly; a fuller elaboration and rationale, or additional (legal/ literature) sources and authorities, can be provided on any issue. These comments then should not be considered exhaustive and we welcome future dialogue with the Committee as their inquiry continues.

2. Technology in Policing

2.1. The police are no different from any organisation seeking to harness technology to improve their effectiveness and efficacy. Indeed, technology has provided marked improvements in policing practice and permitted policing to adapt and modernise. However, the adoption or utilisation of some technological capabilities has also led to serious, and public failures. With the unique role of police, such failures can lead to not just operational defects or inefficiencies, but miscarriages of justice. The police, with their vital public service responsibilities, their unmatched powers over citizens, and their potential influence on individuals, groups and society, have a particular responsibility to ensure that their adoption and use of technology accords with important legal and ethical principles, thus ensuring that policing practices are reliable, useful and legitimate.

2.2. At the outset, we would strongly re-affirm findings from scholarship in Science and Technology Studies and in the Social Studies of Forensic Science that technology cannot be neutral. Instead, **technologies are subject to bias in their development, use, and in the communication of technological capacities and their outcomes** (e.g. in public/policy debates, in considerations

by commissioners of implementing technologies, in the use of data and information produced by technological means).

2.3. These **biases can be unintended and not easily visible**, e.g. arising as an outcome of choices made in choosing baseline data on which to test and train technologies, as is the case in algorithmic/automated decision making for areas such as facial, voice or gait recognition, or in the development of analysis software for the use of advanced DNA analyses such as of mixed traces and for attributes such as appearance, age, ancestry, and familial relationships. It is of vital interest to users and potential beneficiaries of technologies to understand the biases in technologies to be enabled to **address and mitigate negative outcomes** of technology uses (e.g. investigative errors, evidentiary issues, miscarriages of justice and discriminatory/ unfair policing more widely).

2.4. Obviously, police officers, and police forces individually, and collectively (and as part of the wider criminal justice system), rely upon, and use various technologies on a daily basis. The vast majority of instances of technological intervention are unproblematic and confer significant benefits, sufficient at least to outweigh any concerns. **However, this should not give rise to complacency over emerging technologies**, and even the adaptation of current technologies, or the potential for 'mission creep' with existing technologies. In particular, there are technologies that require far greater consideration and scrutiny than may have hitherto been the case prior to the adoption of other technologies. The growing fields of **e-policing** [the use of information and communication technologies] and **biometrics** [patterns of physical and behavioural characteristics unique to individuals and/or categorised groups of people], including digital forensics and cybersecurity, automated facial recognition, social mapping via mobile devices and CCTV, and forensic genetic genealogy, are cases in point.

2.5. Many of these emergent technologies do, or will, rely on collecting, storing, analysing and sharing increasingly large amounts of data. Yet the police (technical, practical and investigative) **capacity to manage Big Data** is slow in emerging and likely to pose challenges for some time, including budgetary ones. Much of the data collected and utilised will also be highly personal and confidential, suggesting significant changes in **the relationship between individual/community and the state** will entail. In particular, emerging e-policing and biometrics technologies have the capacity to become **powerful tools** for policing with **significant impact on civil liberties and human rights**. Technologies cannot be implemented without thorough reflection upon their compatibility within liberal-democratic society.

2.6. Simultaneously, technologies will not necessarily have gone through substantive validation processes required to ensure their safe, reliable, useful and legitimate application in policing. **These technologies remain in the process of 'becoming'**, and as such should not be perceived as reliable and legitimate - due to insufficient operational testing and alignment with civil liberties and human rights (an issue raised in the South Wales police court case on automated facial recognition technology).

2.7. Potential uses need to be subject to deliberation with practitioner, professional, community and academic stakeholders. While the technologies

remain emerging, their **testing/preliminary uses should be decided on a case-by-case basis to avoid negative outcomes** such as public disapproval, loss of confidence or trust in technology and/or in the use of technology by policing, or the 'mission creep' of seemingly reliable technology with long-term adverse effects that will only become visible over a longer period of time with possible impacts upon justice. Such deliberation and engagement needs to be open-ended and not instrumental, it must allow for differences and tensions to be given a forum for articulation and negotiation. A variety of modes of open-ended transdisciplinary engagement with citizens includes Citizens Jury, Citizens' Technology Forum, public symposia with civil society organisations and minority communities.

2.8. Advanced technologies require **specialist training** in both development and deployment stages. This includes the informed interpretation and communication of data and information towards their use as intelligence or evidence. Training should be **developed alongside technological capacity** as tested and standardised expertise is integral to reliability, usefulness, and legitimacy of technology use.

2.9. Investigation into **cultural learning** and how technology is employed over time across a police organisation can offer insight on individual and organisational shifts in terms of how policing tools are understood and (under/over)utilised (including on **the role of expectations and uncertainties in making decisions about technology uses**). This can offer a baseline for work towards realising short-term or long-term benefits of technology uses while addressing limitations. It may also highlight any discriminatory/ unfair applications/ utilisation of technologies, or illuminate any 'unintended consequences'.

2.10. An investigation into emerging technological capacities needs to reflect on whether a technology, service, or technological development should be developed and/or deployed for policing purposes at all, or under what specific circumstances their use may be legitimate. **Technological options may not necessarily offer the best or even appropriate resolution** to addressing social issues, and other options may produce better outcomes. After thorough reflection, the rejection of technological advances should be viewed as a positive outcome, not a 'failure'.

2.11. Developing technologies are imagined to be deployed, subject to different logics: to control crime, to facilitate due process, and to enable surveillance to anticipate threats and support proactive policing. While all three logics overlap and interact, one or another tends to be drawn upon as the key rationale for specific technology uses. It is highly relevant to explore which technologies are imagined/expected to support which aspect/focus of policing and criminal justice, and which logic is drawn upon to, both, make arguments about, and reflect on the usefulness and legitimacy of a technology (on forensic genetics see, e.g., Williams and Wienroth 2017).

3. Accountability & Scrutiny

3.1. There is much scholarship on the vital role of **procedural justice as key to policing legitimacy** (e.g. Hough 2021) and the securing of public confidence

and support. The police cannot function without public confidence and support and it is hard won and easily lost. The use of technology does not diminish the need for procedural justice, in fact, its use should always be gauged by how it will secure and maintain fairness of police processes. Such fairness should always be demonstrable, and the use of technology (including use of data) must be transparent.

3.2. Oversight requires evaluation of the scientific and operational validity of technologies and scientific methods as well as an infrastructure that enables meaningful scrutiny. The use of technology in policing thus requires **robust mechanisms of accountability and scrutiny**. Regulation requires continuous oversight, monitoring, and regulatory structures that are capable of **anticipating as well as responding** to emerging issues. Actors and bodies tasked with oversight roles should be enabled to conduct research and derive rules/guidance. Wherever possible, these should be statutory bodies with sufficient resourcing and powers to be effective. Existing ethics review such as the West Midlands Police Data Ethics Committee, and other jurisdictions such as the New Zealand Police Expert Panel on Emerging Technologies, should be studied to understand their integrated role and oversight capacity, as well as the limitations in their capacity to scrutinise and to hold technology developers, users and commissioners to account.

3.3. While many uses of technology may be justified exceptionally, they should not be considered 'normal' practice until sufficient scrutiny/testing etc. has been undertaken. The onus remains on the state to **justify measures as necessary and proportionate**. This has often not been evidenced prior to, or even subsequent to implementation.

3.4. Independent oversight bodies will need to be also free of any scientific or commercial links to **ensure their impartiality**. It should be expected that there will be significant pressures, and vested interests in seeing a 'positive' outcome of technology evaluation. Any body itself must also be completely transparent, and incorporate multiple diverse perspectives, as well as being given full **access to all necessary data**. Of course, any technology evaluation requires sophisticated data collection from the outset in order to enable later evaluation. There will need to be early agreement on what data points will facilitate evaluation and assurances that such data will be collected. It should be expected that this will include sensitive and complex data, so there must be **early engagement with a pluralist variety of experts** who can bring vital insight to addressing the inevitable practical and ethical issues with the collection of this data.

3.5. Oversight and accountability processes must attend to the **key role of values** in technology use for policing purposes, integrating (1) scientific validation, (2) effectiveness and efficiency considerations, (3) operational needs and capacities (e.g. how does an emerging technology relate to existing practices) with (4) legitimacy and wider integrity aspects of using new, especially data-driven, technologies in policing (e.g. see Wienroth [2020] on **reliability, utility, legitimacy**, and McCartney (2015) and McCartney & Amankwaa, [forthcoming] on **integrity, effectiveness and efficiency**).

3.6. Measures of 'efficiency' and 'effectiveness' must be integrated with broader considerations to achieve both a realistic, and holistic view of technology 'utility'. In 2007, the Nuffield Council on Bioethics published a report on the forensic use of bioinformation, focussing upon those principles to be respected when the State exercises power over citizens, such as the respect of personal liberty; the maintenance of autonomy of the individual; personal privacy; informed consent and equal treatment (Nuffield Council on Bioethics 2007). More recently, Scotland has created a legislative framework for the police use of biometrics, with the Scottish Biometrics Commissioner Act 2020, section 2(1) stating that the function of the new Commissioner is to support and promote the adoption of '***lawful, effective and ethical practices*** *in relation to the acquisition, retention, use and destruction of biometric data for criminal justice and police purposes'.*

4. Select Case Studies

4.1. **Digital spaces**: these enable the police to engage with citizens across spaces and in real-time. Often this means that police services can choose how and when to broadcast information and in doing so can engage with citizens who rarely have contact with the police. Much current evidence indicates that (1) social media is used by the police to communicate information *to* citizens rather than engage in dialogue *with* citizens. This coincides with (2) the scale of social media that by its very nature involves the police speaking to many diverse users, as such communicating more generalised messages rather than addressing specific communities. Emerging research has also shown that (3) police use of social media in digital spaces is interpreted and assessed by citizens in relation to the role and function of the police in physical spaces (Ralph, forthcoming). Above all, this means having a positive encounter and tackling crime in the real world. Consideration should therefore be given to understanding how the relationship between the police and citizens develops over time across physical and digital spaces (in tandem/correlation). This is especially important with police services across the globe increasingly looking to the online world to talk to citizens (see, e.g., Police Scotland's Policing 2026 strategy, National Police Chiefs' Council's Policing Vision 2025 in England and Wales).

4.2. **Data-sharing and cross-database searches**: In 2015, Home Office Strategy and NPCC's Policing Vision 2025 identify data-sharing as one of the strategic priorities for policing in England and Wales, but also for the UK more widely in terms of complex policing concerns around terrorism, organised crime, and vulnerable populations (e.g. domestic abuse and violence). This is a significant element for the coordination and effectiveness of regional and national policing, and concerns not only police force data and data repositories, but also access to, compatibility with, and utility of data from services such as housing, education, social care, health care, etc., in the context of multi-agency policing. However, progress on enabling data-sharing between police databases, and between police forces seems to have stalled, creating practical limits to effective and efficient data-sharing, while multi-agency work is progressing slowly but steadily in English forces. We recommend that two aspects be considered in this area: (1) the practical dimension to data-sharing, including technical capacities, training, and data quality (consisting of validity, reliability, comparability and compatibility of data between police units and forces, as well

as with other services), and (2) the impacts on human rights and social justice as well as on 'policing by consent' that will co-emerge with cross-database searches and the use of traditionally non-policing data for policing purposes. The UK's Biometrics and Forensics Ethics Group has a Complex Data Working Group that engages with some of these issues, and their work would be of value for further enquiry by the IAG.

4.3. **Biometrics**: There is widespread recognition internationally that biometric technologies need careful regulation, with mature and effective oversight and accountability mechanisms, to ensure that trust and confidence in both biometrics and policing are maintained. There is also general acceptance that there are social and ethical consequences to these technologies and the police powers required to utilise them. Often when biometric technologies have been implemented, there have been inadequate justifications for proposals, or a satisfactory evidence base. There have been failures to recognize the legal requirements that must be in place to justify restricting the rights of citizens, resulting in challenges in both domestic courts and the European Court of Human Rights. For the most part, the rights most obviously affected are qualified rights. Under international human rights law, restrictions on these rights, however, must be prescribed in precise and accessible law, and the restrictions in turn must be necessary and proportionate in the particular context, and non-discriminatory. The use of sensitive and controversial techniques (such as forensic DNA phenotyping, forensic genetic genealogy and automated facial recognition), and the impact of mass-retention of biometric data of citizens in large databases, requires further and ongoing interrogation. Questions over whether States are collating and using excessive (sensitive) information of citizens persist, particularly where information could be used for discriminatory purposes, and to the detriment of groups or individuals, which can be unintended and invisible yet still has negative impact. At national level, mass (bio)surveillance of citizens impacts upon the State/citizen relationship. This may occur by stealth, with police powers subtly extended when new opportunities arise for biometric technologies. A coherent and honest assessment and evaluative strategy may be even more vital at a time when other biometric technologies may also attempt to 'piggy-back' on the apparent 'success' of DNA profiling. A realistic and holistic weighing of the benefits brought by forensic DNA profiling necessarily involves reflection upon mistakes of the past, and consideration of whether there is now the foresight, ability, and will, to prevent abuses and over-reach, and augment the advantages of biometric technologies in the future in a viable, ethical and socially acceptable fashion.

4.4. **Automated decision-making** (ADM) (e.g. in automated facial/voice/gait recognition and comparison): There are a variety of ways in which ADM can and has been employed. We focus on its role as a surveillance technology. In this context, ADM can significantly reduce time and required staff in supporting policing tactics and strategy. It can also potentially offer a harmonised approach to decision-making in detection. ADM relies on the use of algorithms. That means it is an invisible technology which is capable of escaping scrutiny. The invisibility here refers to at least two aspects: (1) a potential lack of understanding of the processes (throughput) that turn data (input) into information and intelligence (output), potentially leading to difficulties in understanding and/or challenging automated decisions, and (2) lack of

awareness of decisions being made in the first place. Both aspects require significant research into social and ethical aspects of this technology, as well as into the impacts ADM can have on policing practices and on the role of evidence in criminal trials that arises from earlier uses of ADM, e.g. in the analysis of CCTV and subsequent investigative steps taken.

4.5. **Body-worn video** (BWV) cameras: BWV can capture audio and video of police encounters with the public. They are used increasingly in everyday policing to help with shaping behaviours, e.g. towards reducing the number of assaults on officers, and to provide data for de-briefing of officers and reconstruction of encounters between officers and members of the public. Extant scholarship on BWV offers contradictory views on their effectiveness in shaping behaviour, as well as on their impact on privacy rights, and there is anecdotal evidence that officers have mixed feelings about their use. Further enquiry is necessary in order to understand how and under what circumstances BWV can be usefully deployed, including on training officers in their use; what their value is in providing evidence to trials; and, vitally, what the impact on human rights, criminal justice, social justice, and policing practices may be of BWV use linking up with other emerging technologies such as (automated) facial comparison and (automated) facial recognition.

4.6. **Remotely Piloted Aircraft Systems** (RPAS)/Drones: The use of RPAS can significantly improve the capabilities of police forces, particularly in operations such as missing people searches. However, Police Scotland has previously stated that they will consider using RPAS for other policing functions, such as major events and public order responses, and these are situations in which the privacy of the public may be at risk. The Derbyshire Police force publishing drone footage, of members of the public allegedly breaking lockdown rules, is a recent example of the lack of privacy safeguards associated with police drones. RPAS are a novel technology in policing, and their low visibility can result in public consent being difficult to obtain. There should be clear guidelines on what operations the RPAS will be used for, and human rights impact assessments should be conducted for each of these different types of operations. The existing legal framework is not adequate to protect privacy. The UK Civil Aviation Authority CAP 722 guidelines include a section on privacy and security not directed at police uses but only at civil uses of RPAS. Furthermore, the Air Traffic Management and Unmanned Aircraft Act 2021 regards RPAS as possible tools for committing crimes, suggesting that enquiries into emerging policing technologies need also pay attention to potential approaches to counter measures by the police to the use of RPAS for criminal and other purposes that pose a threat to public order.

5. Commercial Developments

5.1. Technology-based forensic and surveillance services to police are, to a significant degree, provided by commercial entities (e.g. 20% of forensic services used by police forces in England & Wales are of a commercial nature, according to a report by the House of Lords Science and Technology Select Committee [*Forensic science and the criminal justice system: a blueprint for change (3rd Report of Session 2017-19)*]. At the same time, commercially developed services such as facial comparison and recognition (Apple, Facebook) and voice comparison (via consumer banking services) are also further

developed with a view to offering these services to policing and other State agencies. This is one of the key contexts within which any emerging technological developments needs to be considered. This **commercial context gives rise to significant concerns about transparency and governance/accountability**, and makes police vulnerable as 'customers', and subject to budgetary constraints which may impact upon technology use.

5.2. Procurement: The example of the forensic market in the UK has shown how **policing procurement practices can hinder technological development** due to corrosive pricing competition, a focus on low-cost services leading to the loss of research into new and more specialist services. The UK Forensic Science Regulator reports over the past few years have given stark warnings of the impact of commercialisation on the provision of forensic services to police forces.

6. Conclusion

6.1. The 2016 Report '*Forensic Science & Beyond'* by the then Government Chief Scientific Advisor rightly stated that: "*The future of forensic science will require close collaboration between a range of scientific disciplines, entrepreneurs and regulators. Importantly it will require strong public engagement leading to robust democratic decisions about the circumstances – the where, when and how – in which these powerful tools will be employed...*" You could easily transpose *forensic science* in this quote for *technology*. Innovation requires multiple partners and the exploitation of new technologies must be accompanied by rigorous evaluation, which includes answering questions of both effectiveness and legitimacy. All of this must be undertaken within a broader context: *"We can only have the best discussion about innovations if we understand that the discussion must be about both science and values."* (Government Chief Scientific Advisor, Annual Report 2015).

6.2. 'Justice' in its broadest sense must always be paramount in any and all such discussions. To ensure the maintenance of a criminal justice process **respectful of human rights and based upon a socially accepted notion of 'justice'**, technologies and their operationalisation within policing (and their governance) must **respect ethical principles of a pluralist society**. It is rarely disputed that there must be 'balances' struck between crime prevention and resolution and other important values, including the protection of human rights of both individuals and groups. For it is always the case that: "the pursuit of justice means more than simply the resolution and reduction of crime" (Krimsky & Simoncelli 2011:xvii). However, a simple balance between security/safety and privacy is subject to an erroneous assumption that these are part of a zero-sum situation. Rather, **more privacy can mean more security for citizens** (e.g. when data held by the State are leaked, lost, or breached). At the same time, privacy tends to be reduced to an issue of information, when it is highly complex and constituted by a range of aspects including "confidentiality, secrecy, anonymity, data protection, data security, fair information practices, decisional autonomy, and freedom from unwanted intrusion" (US Presidential Commission for the Study of Bioethical Issues 2012, 25). Privacy is one of a range of key liberal-democratic ethical values that are expressions of ongoing deliberation processes. These values include **liberty, dignity, integrity (of body, identity, personal data), and justice** - they should not be subordinated to privacy, or ignored in deliberations.

6.3. Critical engagement is key to ensuring that technological *re*solutions [technology cannot provide *the* solution to a social issue] are fit for purpose, and that users are supported in **understanding the opportunities and limitations of technological resolutions** to policing challenges. We are optimistic that the Committee will take the necessary inter- and transdisciplinary approach to exploring issues. As such, we recommend **drawing on the views and experiences of a variety of publics** (practitioners, regulators, civil society organisations, minority communities, commissioners/users/producers of technology, analysts and commentators from the social sciences, ethics, law et al.) to ensure democratic and well-informed deliberation.

5 September 2021

Authors: ***Dr Matthias Wienroth*** *(Vice-Chancellor's Senior Fellow in Criminology/Sociology) and* ***Dr Carole McCartney*** *(Professor of Law and Criminal Justice) with* ***Dr Delphine Defossez*** *(Lecturer in Law),* ***Ms Angela Paul*** *(PhD candidate in Law), and* ***Dr Liam Ralph*** *(Lecturer in Criminology and Policing) at the Centre for Crime and Policing & the Science and Justice Research Interest Group, Northumbria University*

Focused Bibliography

Hough, M. (2021) *Good Policing. Trust, Legitimacy and Authority*. Bristol: Policy Press.

Krimsky, S. and Simoncelli, T. (2011) *Genetic Justice: DNA Data Banks, Criminal Investigations, and Civil Liberties.* New York: Columbia University Press.

McCartney, C. and Amankwaa, A. (forthcoming) Measuring the effectiveness of forensic DNA databasing, in: Toom, V., Wienroth, M. and M'charek, A. (eds.) *Forensic DNA Profiling Across the Globe: Exploring Practices & Politics of Technolegal Worlds*, Abingdon: Routledge [available upon request]

McCartney, C. (2015) Forensic data exchange: Ensuring integrity, *Aust. Journal of Forensic Science* 47(1), 36-49. https://doi.org/10.1080/00450618.2014.906654

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. http://dx.doi.org/10.2139/ssrn.3812576

Ralph, L. (in press) The dynamic nature of police legitimacy on social media, *Policing and Society*. [available upon request]

US Presidential Commission for the Study of Bioethical Issues (2012) *Privacy and Progress in Whole Genome Sequencing*. Washington, D.C.

Wienroth, M. (2020) Value beyond scientific validity: Let's RULE (Reliability, Utility, LEgitimacy), *Journal of Responsible Innovation* 7(sup1), 92-103. https://doi.org/10.1080/23299460.2020.1835152

Williams, R. and Wienroth, M. (2017) Social and ethical aspects of forensic genetics: A critical review, *Forensic Science Review* 29(2), 147-172. [available online and upon request]

[We would be happy to provide further literature recommendations if useful.]