Independent advisory group on emerging technologies in policing

Legal frameworks and ethical standards workstream report

Final Report

February 2023

Scottish Government
Riaghaltas na h-Alba

Table of Contents

Executive summary

This report sets out the research and views collected by workstream 1 of the Independent Advisory Group (IAG) on Policing and Technology. We have considered relevant legal frameworks in Scotland, legal bases, processes and ethical considerations that Police Scotland use vis-à-vis new technologies, procedures and evidence gathering involving technology issues, lessons learned from past and current use of technologies, and international comparisons and examples which can inform our work.

Police use of technology operates within and spans many spheres of legislation. Here we have focused on the Human Rights Act 1998, Data Protection Act 2019 (in particular Part 3 of the Act which applies to authorities processing data for law enforcement purposes) and the statutory equality duties enshrined within the Equality Act 2010 which have been found to be applicable when considering the impact of technology on Scotland's diverse communities. Mechanisms to address and manage the associated concerns around legal issues and impacts of technology were found to range from legislative guidance, to toolkits produced by organisations, and a range of impact assessments. In Scotland, the Biometric Commissioner Act 2020 is a major statutory intervention into this field of legal frameworks and technological capabilities. More codes of practice, such as that for biometrics in Scotland in the course of implementation, are identified as key to resolving issues about a lack of clarity or proportionality in police technology use.

Ethics takes an important role alongside legal framework. It is challenging to operationalise – and in the domain of policing it can be particularly difficult or contentious. However, the ethics associated with emerging technology in policing can be found to be brought into practical terms through the use of impact assessments (understood to be 'live documents' able to adapt to new knowledge), and through advisory engagement or debate on proposed initiatives through the organisational practise of consultation and panels/forums. Taking more ethical approaches reflects Police Scotland's lessons learned from past experience, and may improve social acceptance of their technology-relevant practices. Force policies, guidance, and training are also able to inform officers and staff about ethical standards and the methods in which behaviour is compliant with bias mitigating efforts. Ethical considerations around emergent technology in police work can relate to ensuring and communicating the legal basis for police use of a technology, but also typically consider how technology reifies or augments power relations. Examples of this could include technology enabled mass surveillance or social sorting, expansion of use cases of technology (i.e. function creep), potential chilling effect on populations, collateral intrusion, and insufficient safeguards surrounding analytical capabilities. Police Scotland has many governance processes in place to address the ethical issues discussed in this section, in order to best serve and protect the communities of Scotland from harm. It will be crucial that independent oversight of these ethics processes and due transparency over them are guaranteed and implemented in order to ensure ethical outcomes.

Digital evidence gathering via and from new technologies remains a challenging subject, especially as regards compliance with human rights and equalities objectives. The implementation of the biometrics code of practice in Scotland is a positive step, and this implementation and its evaluation should inform further how procedures and evidence gathering can be improved further to reflect best practice in human rights, equalities and data protection.

In Scotland, the main areas in which lessons can be learned relating to the adoption of emerging technology relate to the following 6 considerations: (1) How capabilities are communicated by police (to multiple stakeholders); (2) Engagement and consultation; (3) Governance structures and oversight process; (4) Identified legal basis; (5) Effective and matured risk management processes; and (6) Horizon Scanning.

(1) How capabilities are communicated by police (to multiple stakeholders) – it is crucial that communication regarding substantial changes to the nature of police work mediated by technology is clear, publicly facing and speaks equitably to a broad range of publics.

(2) Engagement and consultation – a strong democratic engagement and/or consultation process must be enacted upon in order to gain insights from the communities that a police service works for. In Scotland, if the policing by consent model is to be adhered to, then the public should be involved in changes to the policing system which could change the fabric of society.

(3) Governance structures and oversight process – this area has seen the most amount of positive work in Scotland, whereby robust structures which allow governance processes to be followed and effective oversight to be attained are now frequent features of new change initiatives in Scotland. Learning from past mistakes has allowed for the Memorandum of Understanding to be built which addresses this area.

(4) Identified legal basis – some kind of legal basis assessment must be considered before any new technology is implicated in policing to understand the power which comes from what law which sanction the use of a technology (then for example; proportionality and necessity testing; accurate and reliable/scientific standards, EqHRIA and community impact assessments should follow). This must be clearly communicated to stakeholders and the public.

(5) Effective and matured risk management processes – the continued improvement of a risk management throughout an organisation will be crucial in scoping, mapping, identifying and addressing any risk, opportunity or issue which may become associated with the adoption of a new technology. With a risk-based approach to understanding contexts and stakeholders, there will be greater emphasis placed on considering social impacts of technology and ways to understand how communities will respond to proposals.

(6) Horizon Scanning - Elsewhere around the world, there are also lessons to be learned from similar jurisdiction. The methodology to gain insights in this regard is known as horizon scanning, and will continue to be crucial in knowledge exchange, information on best practice, and the consideration of high risk initiatives which may not be acceptable in Scottish society.

We have devised a number of specific recommendations relating to legal and ethical uses of technology by Police Scotland:

1. The continued implementation and reinforcement of a human rights-based approach to policing in Scotland

Police Scotland should continue to embrace and implement a human-rights based, ethical and proportionate model for police use of technologies, in accordance with international best practices and with community input and engagement.

These international best practices include European Convention on Human Rights and their interpretation by the European Court of Human Rights and should be adhered to by Police Scotland regardless of whether the UK decides to repeal the Human Rights Act and/or leave the European Convention on Human Rights. In such a case, action by the Scottish Government may be required e.g. to incorporate these provisions into Scots law if possible.

This approach should include Police Scotland providing more analysis and engagement of human rights and equalities with technology use; specific references to Police Scotland's duty to assess and review relevant equality impacts of policies on technologies when at a developmental stage. The enhanced human rights-based and ethical approach should take place across the following domains: Policy and strategic decision making; Operational planning and deployment; Training and guidance; Use and control; and Investigation, monitoring and scrutiny. We recommend Police Scotland formally commit to adopting this approach which would ideally be accomplished through further internalising human rights knowledge and capacity. For example Police Scotland could employ equality and human rights experts in order to assist in policy design, analysis and assessment.

2. Further consideration of impacts on new technologies on human rights and equalities needed

The impacts of new technologies specifically on human rights and equalities need to be further considered. A multi-level analysis of rights and equalities impacts should be taken into account to embed and enhance Police Scotland practice, i.e. looking at the impact at the individual, community and societal levels. There are existing requirements under data protection law (Data Protection by Design and Default, Data Protection Impact Assessment) that place an obligation on controllers to ensure that the data protection principles are adhered to and that any impact on individual rights and freedoms are identified, assessed and mitigated. There are also existing relevant obligations under equalities law and human rights legislation. In this recommendation we seek to aid compliance and raise the bar. In terms of raising the

bar from a data protection point of view, specific actions could ensure that: Data Protection Impact Assessments (DPIAs) are developed alongside Equality and Human Rights Impact Assessments (EqHRIAs) and Children's Rights and Wellbeing Impact Assessments (CRWIAs), that Police Scotland refer to the ICO's Overview of Data Protection Harms when considering risks associated with processing and ensure that risks to individual's rights and freedoms are fully considered, assessed and mitigated in DPIAs. Further that these risks should continue to be identified, assessed and mitigated throughout the lifecycle of a new technology (i.e. not only at the 'developmental stage'). From an equalities and human rights perspective, Police Scotland need to assure themselves when undertaking Equality and Human Rights Impact Assessments (EqHRIAs) that any proposals are compliant with the Human Rights Act 1998 and the Equality Act 2010, and also satisfy the requirements of the Equality Act 2010 (Specific Duties) (Scotland) Regulations 2012, including the duty to assess the impact of applying new or revised policy or practice and publishing the results of these assessments in a manner that is accessible.

3. Strong democratic engagement and consultation processes should be used to gain insights from the communities that a police service works for.

These communities should include engagement with the protected groups defined in Equality Act 2010. In Scotland, if policing is to be done with public acceptance and agreement, then the public should be involved in changes to the policing system which could change the fabric of society, effect social relations, or impact democratic values. Complaints processes involving police use of technology must be accessible to all members of the public including those with disabilities.

4. Legal basis for using policing powers vis-a-vis technologies must be clearly specified and shared with key stakeholders

Police Scotland need to be able to demonstrate that the application of the policing power as set out in law must be clear and foreseeable and refer to and use proportionality and necessity testing; accurate and reliable/scientific standards, EqHRIA and community impact assessments. Although Police Scotland do specify the legal basis in DPIAs, given the potential for differing interpretations, legal basis (and opinions being drawn on) should be shared with key stakeholders as a matter of course in order that they may be questioned and tested and this must be reviewed in light of further developments (such as change in use case or additional information coming to light). Police Scotland need to be able to understand and articulate to diverse stakeholders the power which comes from the specific law which sanctions the use of a technology and refer to and use proportionality and necessity testing; accurate and reliable/scientific standards, EqHRIA and community impact assessments. There should be more transparency with regards to the legal basis of police use of technologies and awareness raising with the public.

5. Further clarifications of legal basis via legislation or code of practice may be desirable

Further clarifications of legal basis for police use of technologies may be desirable, such as through legislation or a code of practice as we see for biometrics. Government should consider whether additional statutory codes of practice may be required to provide greater clarity and safeguards on the application of new technologies. Such new technologies might include AI for which a binding code for policing use may be desirable.

6. Special regard for the interests of children and vulnerable persons

When using new technologies in this context, law enforcement actors must have special regard to the interests of children and vulnerable persons and how the technologies may impact upon them. We recommend that Police Scotland conduct, embed and enhance Children's Rights and Wellbeing Impact Assessments (CRWIAs) alongside DPIAs and EqHIAs

7. More communication with the public and other stakeholders about police technology

Communication with the public and other stakeholders is needed about police technology capabilities and substantial changes to the dynamic of police work mediated by technology. This communication must be clear, publicly facing and speak equitably to a broad range of publics. Doing this is important both in terms of understanding and mitigating potential risks and harms but also ensuring fairness. The use of new technologies should not unjustly adversely impact an individual or group of individuals (which may potentially be discriminatory under the Equality Act 2010) and the processing should be within the reasonable expectations of the public.

8. Unacceptably risky technologies

Police Scotland should consider that in some cases a technology may be too controversial and pose unacceptably high risks to use even if there may be a legal basis for using it. A current example may be live facial recognition. Not using certain technologies and applications must be an option. Police and other actors in government should seek to understand why such technologies are considered controversial and risky and draw on lessons learned. Further work needs to be done on how unacceptability of risk may be assessed. Regard could be paid to the EU's proposed AI Act framework for risk in doing this. A category of 'unacceptable risk' could be added to Police Scotland's data ethics process to add to the current low, medium and high risk categories. In addition or as an alternative, the Scottish Government and Parliament could enact legislation defining what unacceptable risk means and designating technologies or application which pose such risks, e.g. those systems whose use is intrinsically incompatible with human dignity (similar to the categorical prohibition of torture).

9. Ongoing evaluations and reflections on police use of technology

Police Scotland should continue to evaluate and reflect on its uses of technologies, recognising lessons learnt and the implementation of measures such as ethics panels, improved internal processes, engagement, transparency and external evaluations.

10. Drone awareness and impact

Police Scotland should raise awareness of its use of drones among the general public, clearly communicate to the general public how and when drones are deployed and how personal data is processed and should publish its draft Code of Practice on the use of drones and impact assessments, including the technical capacity of drone platforms to ensure privacy and data protection by design. Future Scottish Government Crime and Justice Surveys could include questions to benchmark awareness and attitudes of drones. The necessity of drone deployment rather than other means of investigation must be explained and justified by Police Scotland given the likelihood drones will capture sensitive personal data and have a high risk of collateral intrusion. Police Scotland should ensure that drone footage secured in criminal investigations from other parties, whether other public bodies, commercial organisations or others complies with the relevant legal and ethical safeguards.

11. Cross-border dialogues

Police Scotland should look across borders to access and share learning about best practice and acceptable use of new technologies. Evidence collected in trials, risk assessment and ethical studies elsewhere in the UK and further afield may be particularly helpful.

12. Lessons learned forum for police within the UK

A ‘lessons learned’ forum/knowledge exchange event could be established for police in Scotland, along with police in other parts of the UK, to share, showcase and discuss organisational knowledge from previous endeavours. This would mitigate continual institutional failures or mistakes relating to ethical and legal concerns, and allow best practice to be communicated in a transparent and open manner.

13. Continued enhanced risk management

Police Scotland should continue to enhance its approach to ensure effective and mature risk management processes (note link to workstream 4) to scope, map, identify and address any risk, opportunity or issue which may become associated with the adoption of a new technology, and continue to reassess and evaluate risks throughout the lifecycle of any new technology. With this risk-based approach to understanding contexts and stakeholders, there should be greater emphasis placed on considering future impacts of technology and ways to understand how communities will respond to proposals. Evaluating risks throughout the lifecycle of the technology will also allow Police Scotland to act on risks which only become evident after the technology is deployed.

14. Technology procurement and provenance

More attention should be paid to the procurement and provenance of the technologies used by Police Scotland. In order to ensure enhanced cyber- and data security, the police and public sector more widely may need to consider developing technology solutions in-house rather than outsourcing them to private companies. Police Scotland should ensure that there are robust procurement processes in place to ensure that procured technologies are compliant with existing data protection, human rights and equalities obligations. National standards or a national Code of Conduct setting out these standards may be helpful here. Any proposed technology procurement project should follow the HM Treasury Green Book's business case framework, and make public an abridged version which includes an account of ethical issues. Where the police and public sector are developing technology solutions in-house rather than outsourcing to private companies robust design guidance that facilitates a data protection by design and default approach should be in place. A system of independent quality checking of such technologies may be desirable.

15. Police data sharing

More attention should be paid to the sharing of personal data generated by technologies used by police. Further safeguards may be needed for data sharing with other agencies and retention periods. There should be a review of the rules on retention considering questions of utility, lawfulness, proportionality and necessity. Rules around data sharing for the police should be legislated. A separate regime for children's data compared to that of adults may be advisable too. More research and discussion is needed on this topic, with the possible outcomes of further guidance, legislation and/or policy from relevant bodies such as the Scottish Government, Scottish Biometrics Commissioner and the ICO.

16. Biometrics transparency

More information could be published by Police Scotland publicly about biometrics they hold, for instance how many images they hold. The minutes of the Biometrics Oversight Board should also be published.

17. Evaluation of new Biometrics Commissioner

The establishment and effectiveness of the new Biometrics Commissioner in safeguarding human rights and upholding high ethical standards should be evaluated. There is already a reporting mechanism in the Scottish Biometrics Commissioner Act (SBCA) 20202 (section 6). We reiterate the need for this reporting to be done in a way which involves wide consultation with relevant stakeholder groups and the public. We also consider that there should be a review of areas of police technology usage not currently covered by the SBCA, for the consideration of further policy, legislative and guidance reform.

1. Introduction

1.1 This is the report produced by workstream 1 of the IAG on Emerging Technologies in Policing to the Scottish Government. Since its announcement in 2019, the IAG has gathered evidence, views and sought further research and opinions on several topics relevant to the use of technology by Police Scotland. As part of this work, this workstream has focussed on legal and ethical aspects of police use of technology, including existing legal frameworks, good practices both at home and elsewhere, and the role of ethics panels.

1.2 The focus of this report is to discern what factors and what premises Police Scotland should engage when making decisions about using modern technology in policing. In this context, the past five years are of particular interest as there was a significant commitment by Police Scotland in their strategic framework, Police Scotland's Policing 2026 Strategy and its implementation plan, to engage in digital policing and their approach to cyber crime. This resulted in far greater engagement with technology internally and significant external engagement with stakeholders and regulatory bodies. The use by police of all technology within the general computing age engaged challenges of both scope and scale in terms of how police perceived their authority and how that authority was restricted by law and ethics. With incredibly rapid acceleration of technology within the past 10 years Police Scotland has expressed a need to increase their technological capabilities in order to fulfil their statutory role of prevention, detection and apprehension of crime. This involves digital forensics, biometrics; field equipment and information infrastructure, all of which employ the processing of personal data within the meaning of the Data Protection Act 2018. There continues to be an expectation that the accelerating pace of technological advance will place demands upon the Police to employ new, more modern technological solutions and methods. Examples of new technologies include facial recognition software; biometrics, data analysis; robots (including drones); enhanced body-worn cameras; shotspotter; thermal imaging; smarter cruisers; automatic license plate recognition and artificial intelligence to analyse data. This term covers both AI and non-AI tech. We have also seen the establishment of the independent Scottish Biometrics Commissioner, via the Scottish Biometrics Commissioner Act 2020, whose general function is to support and promote the adoption of lawful, effective, and ethical practices regarding biometric data for criminal justice and police purposes.

1.3 This paper considers current police engagement with certain technologies, informed by their history and contemporary commentary. Within the past four years Police Scotland have been challenged and criticised with regard to its knowledge, understanding and implementation of human rights standards to guide its policing. This is in light of its status as a unique public body with a fundamental basis in human rights law (i.e. fulfilling Art 2 of the ECHR, the right to life) as well as its own stated aims and strategy of operating rights-based policing. This critique has come from: Parliamentary committees; National Human Rights Institutions (NHRIs); statutory inspection bodies; and stakeholders.

Tasked with conducting an independent review, Lady Elish Angiolini published two reports in Policing - complaints handling, investigations and misconduct issues: independent review - 2019 preliminary report and Policing - complaints handling, investigations and misconduct issues: 2020 independent review posing some critical questions about the structure of policing infrastructure and its compliance with legal requirements of transparency and independence. On 13 June 2019, the Cabinet Secretary for Justice appeared before the Policing Sub-Committee of the Scottish Parliament to respond to evidence on Police Scotland's proposed use of Digital Triage Devices, known as cyber kiosks. This followed a year of deliberations and investigations into their use, during which Police Scotland were forced to suspend the use of these devices while the Justice Committee's Policing Sub-committee (JCPS) queried the lack of a legal basis for their use. At this appearance the Cabinet Secretary also announced that he would set up an IAG to examine Police Scotland's use of Emerging Technologies, of whose outputs this report forms part.

1.4 Incorporating academic, operational, legal and policy based expertise, this IAG workstream explored the recent history of policing and technology in order to establish the contemporary context. Legal frameworks, both in Scotland and further afield, have been analysed for comparison and specific examples have been cited to reflect the demonstrable impacts of ethical considerations on the role and practices of the police. Police Scotland's own input into this group has provided valuable insight into operational practices and deficits. The breadth of input encompasses open public consultation and specifically commissioned research alongside the professional expertise inherent in the workstream membership.

1.5 This workstream report should be read alongside the other IAG contributions including the final IAG report which this report feeds into. The recommendations that we make, and recommendations that the final IAG report may make, expected to be considered in the context of a fast moving technological landscape.

1.6 From here, we consider legal frameworks, before proceeding to consider processes for considering legal bases for policing, and ethical considerations. We then turn to the issue of digital evidence and procedures for its use in the criminal justice system. Following that, we consider good practices from the UK and elsewhere in the world, and look at lessons learned. We then look to the future, before concluding the report with a series of recommendations.

2. Legal Frameworks

2.1 In this part of the report we consider existing legal frameworks which relate to and intersect with policing and technology: in particular, equalities law, human rights, data protection and policing legislation. We look at the impact that individuals may experience on their rights as a result of police use of new technologies and we consider whether legislation provides appropriate and sufficient safeguards against risks to and impacts on rights, for individuals and communities. We also look at the observed impacts on rights in other jurisdictions given emerging policing technologies. We consider whether existing legislation is fit for purpose especially as regards future developments and whether there are any legislative gaps which need to be filled.

Relevant legal frameworks in Scotland

2.2 There are various legal frameworks relevant to policing and technology in Scotland. Here we cover some of these frameworks; they are also addressed by the research commissioned for the IAG. For example, policing legislation such as the Police and Fire Reform Scotland Act is not covered here in this report.

Human rights

2.3 As part of the UK, which is a signatory of the European Convention on Human Rights (ECHR), Scottish public entities bear the primary duty to promote protect and fulfil human rights enumerated in that document. States have a positive obligation to protect against discrimination and promote equality. The Scottish Government should place human rights at the core of how new digital technologies are used in the criminal justice system. The ECHR has some domestic effect in the UK via the Human Rights Act 1998. Section 6 of the Act makes it unlawful for a public authority to act in a way which is incompatible with a Convention right (an ‘act’ also includes the failure to act).

2.4 Key ECHR rights engaged by the use of new technologies include, but are not exclusive, the following:

- Article 2: Right to life
- Article 3: Freedom from torture and inhuman or degrading treatment
- Article 4: Freedom from slavery and forced labour
- Article 5: Right to liberty and security
- Article 6: Right to a fair trial
- Article 7: No punishment without law
- Article 8: Respect for your private and family life, home and correspondence
- Article 9: Freedom of thought, belief and religion
- Article 10: Freedom of expression
- Article 11: Freedom of assembly and association
- Article 14: Protection from discrimination in respect of these rights and freedoms
- Protocol 1, Article 3: Right to participate in free elections

2.5 Various pieces of domestic legislation are also relevant to implementing these rights, including the protections against discrimination and the Public Sector Equality Duty in the Equality Act 2010.

2.6 The impact and type of right affected is dependent on how new technologies are designed; the purpose and context in which they are used; and the safeguards and oversight systems in place. There are clear human rights obligations that apply in this area derived from the Human Rights Act 1998, and international human rights law, together with data protection and non-discrimination duties that derive from the Equality Act 2010. There is an emerging body of human rights jurisprudence on the development and use of digital technologies and the need to be taken within a human rights framework, this means considering cross-cutting human rights principles such as transparency, non-discrimination, accountability and respect for human dignity. It is also crucial that the private sector meets its due diligence obligations to ensure protection of human rights. Human rights are in place to guard against the risks of misuse and mishandling as well as providing effective remedy.

2.7 The UK Government introduced a bill ('Bill of Rights Bill') to the UK Parliament in mid-2022, whose aim is to replace and repeal the Human Rights Act 1998. The UK would still have remained party to the European Convention on Human Rights, the rights would still have had effect in domestic law and public authorities would still have duties to act in a way compatible with them. However, various reforms would have made it more challenging for claimants to bring cases and would alter how courts interpretation legislation and Convention rights. Overall, it seems that the Bill of Rights Bill would have weaken human rights protections in the UK. The Scottish Government's policy position as of early 2022 was to oppose the UK Government's proposed reforms, on the aforementioned grounds and also given the potential impact on the devolution settlement given compliance with the Human Rights Act 1998 is a condition of the Scottish Parliament passing legislation in the Scotland Act 1998. In September 2022, the new UK Government under Liz Truss withdrew the Bill of Rights Bill.

Data protection

2.8 One key area of legislation is privacy and data protection law. The UK is a signatory to the Council of Europe Convention No. 108 on data protection. Council of Europe Convention No. 108 for the protection of individuals with regard to the automatic processing of personal data, an international treaty on data protection. The UK also has data protection legislation in the form of the Data Protection Act 2018, which implements the most recent reforms to EU law in this area including the General Data Protection Regulation and Law Enforcement Directive, and at the time of writing is still in force. This means that currently UK law reflects EU standards in data protection (and is known as the 'UK GDPR').

2.9 Law enforcement authorities in Scotland are subject to UK data protection law which incorporates the UK GDPR and the Data Protection Act 2018 (DPA 2018).

2.10 Which data protection regime applies depends upon the purpose of the processing and the nature of the body that is carrying out the processing. Part 3 of the Data Protection Act 2018 applies specifically to competent authorities (or their processors) processing for criminal law enforcement purposes. The legislation defines a competent authority as:

- a person specified in Schedule 7 of the DPA 2018; or
- any other person if, and to the extent that, they have statutory functions to exercise public authority or public powers for the law enforcement purposes.

2.11 The Chief Constable of the Police Service of Scotland, Procurator Fiscals and the Crown Agent are specified in Schedule 7. Other Scottish Policing bodies are identified as competent authorities by virtue of their statutory functions.

2.12 Law enforcement purposes are defined under section 31 of the DPA 2018 as:

- *'The prevention, investigation detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.'*

2.13 Part 3, Chapter 2 of the DPA 2018 sets out the main responsibilities for competent authorities processing personal data for law enforcement purposes.

- All processing of personal data for law enforcement purposes should comply with the six data protection principles and must be:
- lawful and fair (first principle);
- collected for specified, explicit and legitimate purposes, and not processed in a manner that is incompatible with the purpose for which it was originally collected (second principle);
- adequate, relevant and not excessive in relation to the purpose for which it is processed (third principle);
- accurate and, where necessary, kept up to date, and every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the law enforcement purpose for which it is processed, is erased or rectified without delay (fourth principle);
- Personal data processed for any of the law enforcement purposes must be kept for no longer than is necessary for the purpose for which it is processed (fifth principle);
- Personal data processed for any of the law enforcement purposes must be processed in a manner that ensures appropriate security of the personal data, using appropriate technical or organisational measures (and, in this principle, "appropriate security" includes protection against unauthorised or unlawful processing and against accidental loss, destruction or damage) (sixth principle).

2.14 Where Information Commissioner's Office list of competent authorities are processing personal data for general purposes (e.g. safeguarding), the UK GDPR

applies. Data protection law is regulated by the Information Commissioner's Office (ICO).

2.15 In June 2022, the UK Government published its UK Government response to the UK Government 'Data - a new direction' consultation which it launched in September 2021, setting out the UK Government's intention to reform data protection law post-Brexit. In July 2022 the UK Government introduced the Data Protection and Digital Information Bill to the UK Parliament, containing various proposed reforms to the current data protection legislative framework. Of note from the policing and law enforcement perspective were the plans to remove: the requirement incumbent on police and law enforcement to log a justification for accessing specific data records; the requirement that individuals must be informed that they have been subject to automated decision-making; and the Biometrics and Surveillance Camera Commissioners and the Surveillance Camera Code in England and Wales. The Bill would also have extended by two months the interval that law enforcement agencies have to respond to access requests. However, a second reading of the Bill in September 2022 in the House of Commons was withdrawn and at the time of writing has not been rescheduled so the Bill's progress is unclear.

Sensitive data

2.16 Information Commissioner's Office clarification of sensitive processing is defined in section 35(8) of the DPA 2018 as:

(a) the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership;
(b) the processing of genetic data, or of biometric data, for the purpose of uniquely identifying an individual;
(c) the processing of data concerning health;
(d) the processing of data concerning an individual's sex life or sexual orientation.

2.17 When undertaking 'sensitive processing', in order to comply with the first principle (lawful and fair) the processing must be:

- based on the consent of the data subject; or
- strictly necessary for the law enforcement purpose and based on a Schedule 8 DPA 2018 condition.

2.18 In practice it is very difficult to obtain valid consent for processing personal data in a law enforcement context because of the high standards required for valid consent under data protection law. This means that in most instances competent authorities processing sensitive data must be able to demonstrate that the processing is **strictly necessary** and be able to satisfy one of the conditions in Schedule 8 of the DPA 2018. Strictly necessary in this context means that the processing has to relate to a pressing social need and that it cannot reasonably be achieved through less intrusive means. Competent authorities will also need to ensure that there is an appropriate policy document in place. The conditions for sensitive processing in Schedule 8 of the Act are described on the ICO website.

Automated decision making

2.19 A data subject has the right not to be subject to a decision that is:
- based solely on automated processing; and
- produces an adverse legal effect or significantly affects the individual;

2.20 Unless that decision is required or authorised by law.

2.21 Section 50 of the DPA 2018 sets out the legal obligations placed on competent authorities when using automated decision making. These include making sure that individuals are able to:
- obtain human intervention;
- express their point of view; and
- obtain an explanation of the decision and challenge it (the obligation is to inform the data subject in writing that they have been subject to a decision based solely on automated processing).

2.22 As mentioned earlier, the Data Reform and Digital Information Bill proposes to remove the requirement that an individual is informed about automated decision making being used vis-a-vis them in the policing context.

Data protection impact assessment

2.23 Controllers must carry out a data protection impact assessment (ICO definition of (DPIA) before they process personal data when the processing is likely to result in a high risk to the rights and freedoms of individuals.

2.24 Processing that is likely to result in a high risk includes (but is not limited to):
systematic and extensive processing activities, including profiling and where decisions that have legal effects, or similarly significant effects, on individuals;
large scale processing of special categories of data or personal data relation to criminal convictions or offences;
using new technologies (for example surveillance systems).

2.25 Controllers must take into account the nature, scope, context and purposes of the processing when deciding whether or not it is likely to result in a high risk to individuals' rights and freedoms.

2.26 It is good practice to carry out a DPIA for all new processing. Undertaking a data protection impact assessment (or DPIA) can help controllers identify the most effective way to comply with their data protection obligations and meet individuals' expectations of privacy. An effective DPIA will allow controllers to identify and fix problems at an early stage, reducing the associated costs and damage to reputation which might otherwise occur.

2.27 When undertaking a DPIA, the ICO recommends that controllers refer to its Overview of Data Protection Harms and the ICO's Taxonomy to help them identify possible harms that may arise from plans that are being considered.

Data protection by design and default

2.28 Under the UK GDPR and Part 3 of the Data Protection Act (Section 57), controllers have a general obligation to implement appropriate technical and organisational measures to show that they have considered and integrated the principles of data protection into its processing activities.

2.29 If a controller is processing personal data for law enforcement purposes it must implement these measures by default to ensure that it only process personal data for a specified and necessary purpose.

2.30 It must also ensure that by default it has put safeguards in place to prevent personal data being made available to an indefinite number of people without an individual's intervention. The ICO has published guidance on privacy by design and default within the Guide to the UK GDPR.

Artificial intelligence guidance

2.31 The ICO has guidance on AI and data protection that it recommends controllers take into account in formulating plans to process and actual processing of personal information that involves AI. This guidance is best practice for data protection-compliant AI, as well setting out how it interprets data protection law as it applies to AI systems that process personal data. It contains advice on how to interpret relevant law as it applies to AI and recommendations on good practice for organisational and technical measures to mitigate the risks to individuals that AI may cause or exacerbate.

2.32 In cases where a controller is both using AI and undertaking data analytics, the ICO recommends that it consult its Toolkit for organisations considering using data analytics. The toolkit is most helpful to controllers at the beginning of any data analytics project lifecycle. It will help them to recognise some of the central risks to the rights and freedoms of individuals created by the use of data analytics.

Equality Act 2010

2.33 The Equality Act 2010 (EA 2010) protects individuals from discrimination and supports progress on equality. The Equality and Human Rights Commission has published guidance on the EA 2010.

Non-discrimination

2.34 The EA 2010 provides protection from discrimination, victimisation and harassment because of a protected characteristic. There are nine protected

characteristics – age, disability, gender reassignment, marriage and civil partnership, pregnancy and maternity, race, religion or belief, sex and sexual orientation. The EA 2010 prohibits:

- Direct discrimination
- Indirect discrimination
- Discrimination arising from disability
- Failure to make reasonable adjustments for disabled people
- Harassment
- Victimisation

The public sector equality duty (PSED)

2.35 The PSED is made up of the general duty and specific duties. The general duty requires public bodies to have due regard to the need to eliminate discrimination, advance equality of opportunity and foster good relations between different groups when they are carrying out their activities (see section 149 of EO 2010). The broad purpose of the general duty is to integrate equality considerations into the day-to-day business of public bodies. Not ensuring consideration of equality can lead to unintentional unlawful discrimination, greater inequality and worse outcomes for particular groups of people in our communities. For these reasons, the general duty requires public bodies to consider how they can positively contribute to the advancement of equality and good relations. It requires equality considerations to be built into the design of policies and practices and the delivery of services, and for these to be kept under review. The Scotland-specific equality duties contained in the Equality Act 2010 (Specific Duties) (Scotland) Regulations 2012 (as amended) help listed public bodies meet the general duty. The Equality and Human Rights Commission has also issued guidance on the PSED for Scottish public bodies.

2.36 Scottish Ministers, Police Scotland and the Scottish Police Authority have legal obligations under the PSED as service providers and employers. Of particular relevance when considering the adoption and application of new technologies is the specific duty requirement to assess the equality impact of proposed and revised policies and practices (see regulation 5 of the Equality Act 2010 (Specific Duties) (Scotland) Regulations 2012 as amended). There is guidance for public bodies on how to carry out an equality impact assessment.

2.37 At the earliest stage of the development of a proposed policy or the revision of an existing policy, public bodies should:

- Identify if, and how, the duty applies
- Collect equality evidence
- Assess the potential impact by considering whether the equality evidence indicates potential differential impact on each protected characteristic group or provides an opportunity to improve equality in an area, by asking:
    - Does the proposed policy eliminate discrimination?
    - Does the proposed policy contribute to advancing equality of opportunity?
    - Does the proposed policy affect good relations?

- Take account of the results of the assessment in developing the proposal
- Ensure decision makers have due regard to the results of the assessment when making the final decision about the policy and its implementation
- Document decisions and how due regard formed part of that decision
- Publish results of the assessment
- Monitor the actual impact of the policy

2.38 Also of relevance when considering the adoption of new technology is the specific duty requirement to consider the use of equality award criteria and conditions in relation to public procurement. The EHRC has procurement guidance for Scottish public authorities in order to assist with compliance with this duty.

2.39 On a practical level, Police Scotland need to make sure they have the systems and processes in place to:

- gather and use the equality data of employees in order to meet the requirements of the Equality Act 2010 (Specific Duties) (Scotland) Regulations 2012 (as amended)
- collate and use the equality data of service users as a means of demonstrating compliance with section 149 of EO10

Biometrics

2.40 Biometric data is personal data that is obtained through specific processing relating to physical, physiological or behavioural characteristics of a person. Biometric data is processed "for the purpose of uniquely identifying a natural person" is sensitive data under the DPA 2018.

2.41 There are specific legal regimes related to data protection for biometrics data in the criminal justice system in Scotland. The Scottish Biometrics Commissioner Act 2020 defines biometrics data and set up an independent public body for promoting and support the legal, ethical and effective acquisition, retention, use, and destruction of biometric data for criminal justice and policing purposes in Scotland applies to Police Scotland, the Scottish Police Authority (SPA), and the Police Investigations and Review Commissioner (PIRC). The use of biometrics is supplemented by other legal frameworks, including:

- Equality Act 2010 (Specific Duties) (Scotland) Regulations 2012
- Part 2 of the Criminal Procedure (Scotland) Act 1995
- Section 56 of the Criminal Justice (Scotland) Act 2003
- Chapter 4 of Part 4 of the Age of Criminal Responsibility (Scotland) Act 2019.
- Police and SPA Codes of Practice

2.42 It is important to note however that the definitions of biometric data under data protection law and under the Scottish Biometrics Commissioner Act 2020 (SBC Act) are slightly different. The definition under the SBC Act is broader and includes photographs.

2.43 The SBC has a statutory duty to prepare, and from time to time revise, a code of practice on the acquisition, retention, use and destruction of biometric data for criminal justice and police purposes. The Code of Practice will apply to Scottish legislation which permits the capture of biometric data in Scotland by Police Scotland, the SPA or PIRC without consent, except where that data is collected under legislation reserved to the UK Parliament, and where it already falls within the independent oversight of another commissioner. In May 2022, the draft Code of Practice was laid before the Scottish Parliament for comments as required by the SBCA. The Scottish Government will prepare draft legislation on the Code of Practice by the end of 2022. The Code of Practice provides a high-level summary of the 12 Guiding Principles and Ethical Considerations when acquiring, retaining, using, or destroying biometric data for criminal justice and policing purposes in Scotland, Police Scotland, the SPA and PIRC must adhere to the following 12 General Guiding Principles and Ethical Considerations:

- Lawful Authority and Legal Basis
- Necessity
- Proportionality
- Enhance public safety and public good
- Ethical behaviour
- Respect for the human-rights of individuals and groups
- Justice and Accountability
- Encourage scientific and technological advancement
- Protection of children, young people, and vulnerable adults
- Promoting privacy enhancing technology
- Promote Equality
- Retention periods authorised by law

Impacts

Human rights impacts

2.44 Human rights impacts depend on the type of technology used. The range of technologies employed also highlights that it is insufficient to assess the human rights impact of discrete technologies in isolation, but they must also be examined in context and in relation to the overall impact their use has on a particular sector, such as policing. Human rights impacts are also explored by the research commissioned by the IAG.

2.45 New technologies are used in innovative manners to help police to prevent or resolve crime. However there are some human rights concerns. The paper highlights a number of examples, including algorithms, facial recognition software and predictive policing. There is no requirement of independent quality check attached to these technologies at the moment.

2.46 In some cases it may be impossible to know the full impact of police use of technology on human rights, and the harm may be difficult to quantify, particularly as it may continue in the future. For example, when biometric data is collected it is not

transparent to know what will be done later with the personal data (deleted, shared or sold). Consideration should also be taken into account of the impacts and threats of technology use at multiple levels: some technologies and their applications may impact more on the individual, community and society-wide levels.

2.47 In practice, governments often rely on private contractors to design and develop new technologies in a public context. This is also true of the police. Private actors should comply with all applicable laws and respect human rights. We have a collective responsibility to give direction to these technologies so that we maximize benefits and curtail unintended consequences and malicious uses.

2.48 Discrimination can result from the design and development of digital technologies. AI and machine learning systems are often dependent on historic data, which may be incomplete or contain bias. The result is a biased technology as such discrimination may then be reproduced and amplified when used by the police.

2.49 The regulation and governance of the design and development of new technologies is therefore critical to create the conditions for innovation and to ensure that these technologies, particularly AI are used to advance, rather than put at risk, equality and human rights. Understanding the multi-level impacts of new technologies, as mentioned, is key, as some of the risks may occur at a more societal level, especially to freedom of association or assembly where a chilling effect may be produced.

2.50 Indeed, risks to democratic freedoms (impacting Articles 9 – 11 of the ECHR) can arise from the widespread use of surveillance tools and AI-enabled technologies by police. There is an increased use of digital surveillance tools in the context of peaceful assembly and freedom of expression under the auspices of national security or public order. This type of interference with our democratic freedoms should only be permitted if it is lawful, proportionate and necessary on a targeted basis where reasonable suspicion can be demonstrated. The proportionality principle requires that any surveillance measure used should be the least invasive option. UK surveillance laws including the Investigatory Powers regimes applicable to certain bulk surveillance practices, must respect these principles. Surveillance practices, bulk data collection and facial recognition technologies employed at large events therefore raise human rights (proportionality) concerns as well as being potentially discriminatory. This was confirmed by the ECtHR in the *Big Brother Watch v. the UK* and *Centrum för Rättvisa v. Sweden* cases regarding bulk surveillance. The issues around facial recognition have been considered in the UK context by the ICO in its Opinion on The use of live facial recognition technology in public places. Furthermore, the *Bridges/South Wales Police* case also sheds further light on the issue (discussed below).

2.51 The principles of equality and non-discrimination are central to human rights law. As discussed, discrimination can be reinforced by AI. It is important that police do not use broad profiles that reflect unexamined generalisations and/or stigmatisation. For example, the use of live facial recognition technology poses a risk not only to the enjoyment of the right to peaceful assembly but also reinforces

discrimination. Those who are particularly at risk of discrimination by this technology include African descendants and other minorities, women and persons with disabilities. For example, there is ample literature on the algorithmic error rate in facial recognition technologies, leading to minority individuals being wrongly flagged leading to detention.

2.52 Currently in Scotland there is a moratorium on police use of live facial recognition technology, which contrasts with the situation in England and Wales, where live facial recognition technology has been deployed by police forces in public places, often in controversial ways and settings. Indeed, a specific use of public space facial recognition surveillance by the police in other UK jurisdictions (England and Wales) has deemed unlawful in the *Bridges v South Wales Police* case from 2020 - although this only declared that particular use of live facial recognition illegal, rather than all live facial recognition use by police. However, non-live facial recognition is used by Police Scotland, which may still exhibit discriminatory biases. Furthermore, live facial recognition has been used by other public agencies in Scotland, such as schools, in controversial ways.

2.53 For biometric data, steps are being taken to clarify the legal frameworks governing its use. The SBC draft Code of Practice, once assented by the Scottish Parliament, will become the first of its kind and Scotland will become the first UK nation to have detailed legislation, a statutory Code of Practice on the acquisition, retention, use and destruction of biometric data for criminal justice and police purposes.

Data protection impacts – A view from Police Scotland

Since 2018, PS has worked to make the use of DPIAs systemic within PS for all new or updated processing, which includes but is not limited to the introduction or use of new technologies. Over 140 DPIAs have been approved since 2018 with more in progress. To underline the value and importance of the DPIA framework:

- PS project 'stage gates' include DPIAs as a mandatory requirement
- PPAs (Pre Project Assessments) are sent for consultation to a range of business areas, including CDO. This allows for early and indicative comments to be provided that will guide PS on the high-level challenges that may be faced by a project.
- Engagement and collaboration with Strategy and Innovation, including regular consultation at the CDO IA team's DPIA meeting. This allows potential technologies to be discussed ahead of any formal documentary submission and consideration given to early steps to be taken.

Police Scotland consider that their impact assessment procedures are aligned in ways which ensure ethical and legally compliant outcomes: that the questions in, and outcomes from a Police Scotland DPIA and EQHRIA are in concert with each other. For example, a DPIA is unlikely to be approved if an EQHRIA identifies negative impacts of technology on a particular section of society. In such examples, the DPIA and EQHRIA frameworks are used to inform and guide the design of processes and processing.

'Adjustment' of technology by police to ensure compliance with legislation can result in a range of different actions. The approach taken by PS is to use the framework of questions in a DPIA to guide the design, build and implementation/use of technologies and processing and therefore, information specialists, SMEs and operational leads work collaboratively to discuss risks and identify solutions. In practical terms this means that a DPIA may go through many draft versions and identify risks for which a project must determine and implement an action plan to allow a risk to be mitigated to the extent that a DPIA can be formally agreed by a Strategic Information Asset Owner (SIAO).

To give the IAG - and wider public - assurance that this process works in practice, Police Scotland gave us a list of examples of changes made to technologies during the proposal/design/development phase in a DPIA framework to ensure compliance:

- The re-design of technical capabilities (common throughout ICT projects)
- PS did not purchase/implement all technological capabilities (cyber kiosks)
- PS agreed not to use technology for a particular purpose (Telematics, LBM) or only after certain authorisations are given and provided privacy notices to that effect
- Contractual specifications (no processing outside of the UK is permitted)
- Additional security controls or configurations
- Testing & POC on dummy data

2.54 Police Scotland may wish to consider including undertaking Children's Rights and Wellbeing Impact Assessments (CRWIAs) alongside DPIAs and EQHRIAs to inform and guide the design of processes and processing as a way of further embedding rights and enhancing the human rights approach of Police Scotland.

Equality impacts

2.55 Police forces may use technology to identify where specific crimes may occur, crime solvability, and who may commit crimes. These technologies are based on predictive analytics which leverages data, algorithms, and other technologies (e.g. facial recognition technology) to monitor and assess individuals, communities and/or specific locations. This type of policing is particularly challenging as it can target particular protected characteristic groups over others, including racial groups, younger people, disabled people, religious groups and women. Both EHRC and SHRC raised concerns in 2020 about potential discrimination caused by predictive policing.

2.56 Police Scotland must harness their EHRIA process to further help them identify potential discrimination and identify opportunities to promote equality when designing, commissioning or using new technologies. From an equality perspective, this means considering the possible impacts the technology can have on people with protected characteristics, thinking about any relevant inequality they experience, barriers or specific needs.

Summary of section

2.57 Police use of technology operates within and spans many spheres of legislation. Frameworks related to technology enabled policing in Scotland could implicate human rights through the Human Rights Act 1998, or issues related to privacy and data protection as per the Data Protection Act 2018 (in particular Part 3 of the Act which applies to authorities processing data for law enforcement purposes, and data protection principles more generally). Furthermore, there are statutory equality duties enshrined within the Equality Act 2010 which have been found to be applicable when considering the impact of technology on Scotland's diverse communities. Mechanisms to address and manage the associated concerns around legal issues and impacts of technology were found to range from legislative guidance, to toolkits produced by organisations, and a range of impact assessments.

2.58 Technological capabilities and associated legal frameworks can both be observed to be always evolving. Sometimes both phenomena are evolving in tandem as illustrated by the Biometric Commissioner Act 2020; and sometimes there may be friction or tension between the developments. What is clear is that neither technology nor legislation exist in a static state. This requires the recurring and iterative need to reconsider and evaluate the impacts of technology on individuals, communities, and society.

3. Processes & ethical considerations

3.1 In this section we further consider the processes and ethical issues in police use of technology. We focus again on processes for establishing legal basis and other tools such as impact assessments. We look more broadly at the notion of 'ethics' in Scottish policing, including the role of ethics boards.

Policing practices, processes and legal bases: A view from Police Scotland

Police Scotland (PS) primarily uses the established frameworks of a Data Protection Impact Assessment (DPIA) and Equality and Human Rights Assessment (EQHRIA), under the Data Protection Act 2018 and the Equality Act 2010 respectively, to establish, define and document the legal basis it relies on for the use of new technology.

Police Scotland assert that for them, a DPIA is not simply a 'checklist document' to be completed by a project ahead of implementation. Rather, it is treated as a framework of questions that when fully answered will allow projects introducing new technologies (as well as a wider range of new or alternative processing) to fully consider the legal basis for that new technology as well as designing the necessary legislative and regulatory compliance into it.

The legal basis for new technology is at the heart of a DPIA, addressing the legislative requirement that processing must be both legal and fair. Police Scotland have learned that an *indicative* legal basis can be established early in the assessment process, generally based on a particular piece of legislation that either obliges or permits an action/task/service. According to Police Scotland, legislation and regulation are however rarely explicit in defining how an action/task/service is undertaken which allows for the evolution of service provision though new technology among other things.

Police Scotland must test an indicative legal basis, such as those defined in the Police and Fire Reform (Scotland) Act 2012, ethical, equality and public opinion considerations. These elements are necessary to make an assessment of 'fairness' and proportionality and as a consequence more work is now undertaken at a granular level to ensure that the legal basis can be both understood and explained in detail internally and externally.

For Police Scotland to come to a decision about a legal basis, this can involve a range of specialisms including but not limited to Operational SMEs, Chief Data Office (CDO), DPO, Legal Services, external consultation groups, SPA and Ethics panels before a final recommendation is made to, and decision taken by, a member of the Force Executive acting as Strategic Information Asset Owner. This is done in the formal DPIA document. As an example, the collaborative work undertaken with the

Advisory Groups for Cyber Kiosks and engagement with the ICO on that technology set the base standard within PS that we now expect in relation to understanding and explaining the legal basis underpinning complex new technologies or innovative processing.

In Police Scotland assessing the legal basis for emerging technologies, it is important to separate decisions about the purpose and the manner of processing. This may appear counter-intuitive because technology may be facilitating a change, however if focus is lost on the purpose and outcome that PS is seeking and is concentrated on the proposed technology, we run the risk of becoming a technology-driven organisation, rather than one that has a policing purpose and outcome at its core.

Realistically, this can mean that the purpose of processing – the 'why/what' - may have a legal basis, however a proposed emerging technology – the 'how' - may not, or it may need development and amendment to be compliant with both primary and secondary legislation and ethically valid. The development or amendment that is required to technology may not however always be a technical one as highlighted in the earlier paper; procedural and behavioural controls can be options for consideration.

The objective legal basis for any processing (and technology) must first have a basis in operational policing/business and the legislation that underpins it. Technology should be facilitative, providing a method of delivering an outcome, but is not an end in itself. Therefore, when a proposal for new technology arises, PS must be able to determine and define the legal basis for the operational purpose and outcome sought that it wishes to apply the technology to. The learning experience from the Cyber Kiosks showed that PS needs to be able to express the fundamental legal basis for its purpose, outcome and operational activity more clearly in order to then best use technology to deliver those purposes, outcomes and operational activities.

The legislative provisions that Police Scotland relies upon as legal bases are many and lengthy and will be based on each purpose, operational activity and outcome. Many of the legislative provisions that underpin operational activities are embedded in Force Standard Operating Procedures (SOPs), Guidance and Training products but are not always bespoke or aligned to a particular technology. Whilst the Police and Fire (Reform) Scotland Act 2012 forms a backbone to many police activities, it is only one element in a much wider legislative remit of tasks either required of the Force, or which it is permitted to undertake. These are not limited to 'policing' activities, but also include the 'corporate' management of the organisation. In addition, there are a range of common law powers that officers will rely on to carry out their duties.

Body Worn Video (BWV) devices can provide prosecutors with high quality evidence to support investigations and prosecutions. Furthermore, they support investigations by Police Scotland and the Police Investigations and Review Commissioner (PIRC) in respect of investigations concerning the policing response to a particular matter. There are recognised privacy, data and policy concerns. To anticipate and mitigate

against potential privacy and third-party concerns, Police Scotland completed a full Equalities and Human Rights Impact Assessment (EqHRIA), and Data Protection Impact Assessment (DPIA). Impact assessments are treated as live documents and therefore reviewed or updated annually to reflect changes in legislation, policy and technology. Police Scotland have also developed and published a detailed Code of Practice which outlines how BWV will be used by armed policing.

Legal bases and processes – Wider views

3.2 While Police Scotland have outlined the approach they take to establishing a legal basis for their technology-related activities above, others consider that there is a lack of clarity or even insufficient legislation in Scotland to facilitate and justify police use of technologies, especially ones which are currently emerging.

3.3 There has been significant controversy and disagreement among stakeholders in Scotland about whether there is an appropriate basis for Police Scotland to use cyber kiosks: Police Scotland has claimed that the legal basis exists, but others such as the Scottish Human Rights Commission were of the view that there is an insufficiently clear legal basis for this. The extraction of data from devices remains a live issue, and is the subject of a new draft code of practice from the UK Government. Although Police Scotland do specify the legal basis in DPIAs, given the potential for differing interpretations, legal basis (and opinions being drawn on) should be shared with key stakeholders as a matter of course in order that they may be questioned and tested and this must be reviewed in light of further developments (such as change in use case or additional information coming to light).

3.4 Further controversies may arise given the lack of clear and explicit legal framework and policy guidance for other technologies such as: facial recognition technologies; unmanned aerial systems/vehicles (drone); body worn cameras; data driven analysis, AI systems and the use of the personal data collected and processed by these technologies. The ICO has produced guidance on a number of these issues including live facial recognition use by law enforcement and more generally in public places, the use of video surveillance, and on AI and data protection. The June 2022 Independent Review of the governance of biometric data in England and Wales ('the Ryder Review') has recommended that a legally binding code of practice for live facial recognition use should be formulated, with a specific code for police use and another code which regulates other uses of live facial recognition. Until those are in place, the use of live facial recognition should be suspended.

3.5 Data-sharing by the police with other agencies may also give rise to concern, which may impact negatively on human rights. There is insufficient knowledge of the extent of such data sharing in Scotland, but in England there have been reports of disabled people who were allegedly photographed by English police forces at an

Extinction Rebellion protest and their details passed to the Department of Work and Pensions. Human rights standards prohibit collection of personal data to intimidate participants in a protest.

3.6 The police play a key role in the task of investigating allegations of criminal behaviour. This includes a number of activities with technological implications such as carrying out searches, undertaking surveillance (e.g. collecting facial images), interrogating suspects and witnesses, and generally securing evidence (e.g. collecting DNA and fingerprints) – triggering the application of Articles 5, 6 and 8 of the ECHR, and which may result in unlawful discrimination under the EA 2010. National and international courts have found violation of human rights in the blanket retention of biometric data: DNA profiles (cellular samples and fingerprints and custody photographs) and bulk surveillance of the public.

3.7 The recent investigation by the House of Lords Justice and Home Affairs Committee into how advanced technologies are used in the justice system in England and Wales led the Committee to be, 'taken aback by the proliferation of Artificial Intelligence (AI) tools potentially being used without proper oversight, particularly by police forces.' The Committee acknowledged that AI offers a huge opportunity to better prevent crime but stressed there is also a risk it could exacerbate discrimination. In the Committee's view, 'without sufficient safeguards, supervision and caution, advanced technologies may have a chilling effect on a range of human rights, undermine the fairness of trials, weaken the rule of law, further exacerbate existing inequalities and fail to produce the promised effectiveness and efficiency gains.' In July 2022 the UK Government released a policy paper, *Establishing a pro-innovation approach to regulating AI,* in which it considers that any regulatory activity should be directed towards AI presenting 'real, identifiable, unacceptable levels of risk', but for now it does not consider legislation to be necessary; instead it plans to introduce a set of non-statutory cross-sectoral principles on AI.

3.8 The Scottish Government launched its own AI Strategy in March 2021, in which it set out its vision to become 'a leader in the development and use of trustworthy, ethical and inclusive AI'. There is no mention of police use of AI in the paper. The Scottish Government has also set out its vision to be an 'Ethical Digital Nation' and behave in ways which generate trust among the public in the use of data and technology. Again, policing/law enforcement are not mentioned in this strategy.

ETIAG public consultation

3.9 A Call for Evidence was issued as part of the IAG's activities. Some responses received discussed ethical and legal dimensions in which two mechanisms were offered to address complex challenges relating to ethical standards. A breadth of responses discussed the utility of both an 'Ethical and legal assessment framework' and an 'Ethics panel' to inform a nuanced and multifaceted

discussion surrounding police use of emerging technologies on a case-by-case basis.

3.10 Many responses identified that introducing technology into operational domains without proper ethical and legal frameworks to engage critical assessment or external consultation, will likely result in negative outcomes for all stakeholders. These potential risks were noted to include: eroding public trust; fostering feelings of oppression and surveillance; increasing more marginal forms of discrimination and violence (including non-violent discrimination and bias motivated violence). These assessments are also understood to allow analysis into equality and human rights impacts of proposed technology. Furthermore, it was emphasised that the legislative framework in which a technology is operating must be well-defined and have exact parameters before technology is introduced. A strong ethical and legal assessment framework would likely mitigate legal, jurisdictional, and operational challenges from transpiring.

3.11 Another mechanism which was frequently noted was an 'Ethics panel'. These forums can allow subject matter experts from a range of disciplines to independently grapple with the ethical and legal issues associated with emergent policing technologies. Practitioner, professional, community and academic voices were recommended to be included on such forums. It was strongly suggested by one response that ethics panels should include people who understand the power asymmetries in the use of technologies.

3.12 Ethics panels were also assumed to be a space which did not include individuals or groups with financial interests, as this was thought to influence decision making which would inform public policy.

3.13 Both the assessment frameworks and ethics panels, it was suggested, should embrace an equality and human rights-based approach to understand impacts on individuals (including witnesses, victims, suspects, members of the public and protected characteristic groups). Outcomes of both of these assurance mechanisms should provide strong and unbiased evidence, prior to its real world implementation, that the proposed technology is non-discriminatory and will not further entrench existing inequalities and explain why it is necessary and proportionate.

Ethics advisory panels: A view from Police Scotland

In addition to the formal governance channels outlined above, Police Scotland have introduced Ethics Advisory Panels (EAPs) to provide an opportunity for staff, officers and external participants to come together and discuss ethical dilemmas within Police Scotland.

Police Scotland's operating model includes a four tier structure of panels. Ethics panels are not decision making bodies, but are instead advisory in nature and provide advice and support to the decision maker. The decision maker (or dilemma holder) remains responsible for taking the decision with due consideration of the panel's views within their rationale.

Ethics panels have a number of objectives. These include: (i) improve service delivery; (ii) support police officers and staff; (iii) support police leaders; (iv) develop and enhance visible ethics culture and (v) support organisational learning.

It should be noted that Ethics Advisory Panels will consider a whole range of ethical dilemmas, not just those posed by the adoption of new and emerging technology.

Below is a brief description of the four tier structure of panels (see Figure below for illustration):

- **Regional Panels** - 150 staff and officers across Police Scotland are trained to sit on Regional Panels. These panels are planned to meet every three months in the East, North and West Regions. Each panel will comprise 15-20 staff and officers and are chaired from a cadre of senior officers and staff members trained for the role. Regional Panels ordinarily consider ethical dilemmas which impact upon local and/or operational decision making with Subject experts (if required), staff associations, unions and human resources represented. Recent examples of subjects discussed at a Regional Panel include Body Worn Video and Gifts, Gratuities, Hospitality and Sponsorship.
- **National Panel** - 50 senior officers and staff members are trained to sit on National Panels. Membership includes those who have a national remit, representatives from staff associations, unions and human resources in addition to representatives from the Regional Panels. As the last tier of panels yet to formally sit, their timetable will align with Regional Panels sitting quarterly, chaired from a cadre of senior officers and staff members trained for the role. The National Panel is intended to consider ethical dilemmas which impact upon national, strategical and tactical decision making across most, if not all of Police Scotland. National panels will also act as a governance route for potential further discussion around dilemmas discussed at Regional Panels.
- **Independent Panel** - Currently 30 members are drawn from a broad spectrum of society in Scotland, with development ongoing to establish a cadre of 35-50 individuals. The Independent Panel will consider dilemmas that impact public service and confidence, providing external consideration, scrutiny and advice to the decision maker. Panels can be convened with 4 weeks' notice on a demand led basis and are chaired by an Independent Member with DCC Professionalism holding the position of co-chair. Recent examples of subjects discussed at the Independent Advisory Panel include Remote Piloted Aircraft Systems (RPAS), the Domestic Abuse Scotland Bill and Body Worn Video
- **Youth Panel** - Working in partnership with the Scottish Youth Parliament (SYP) the Youth panel was established in April 2021 with a trained cadre of 15-20 MSYPs engaging the voice of Scotland's young people in police decision making. The panel is scheduled to sit 3 times a year and will consider dilemmas that impact public service and confidence. The Youth Panel sits parallel to the Independent Panel, ensuring that the diverse and representative democratically elected voice of Scotland's young people is heard. Youth panels are independently chaired by the Convener of the SYP's Justice Committee with CI

Ethics and Preventions holding the role of Police Scotland Delegate on the panel. The first subject discussed at the Youth Advisory Panel was the policing of COP26 with a future dilemma around the implementation of the UNCRC Bill scheduled.

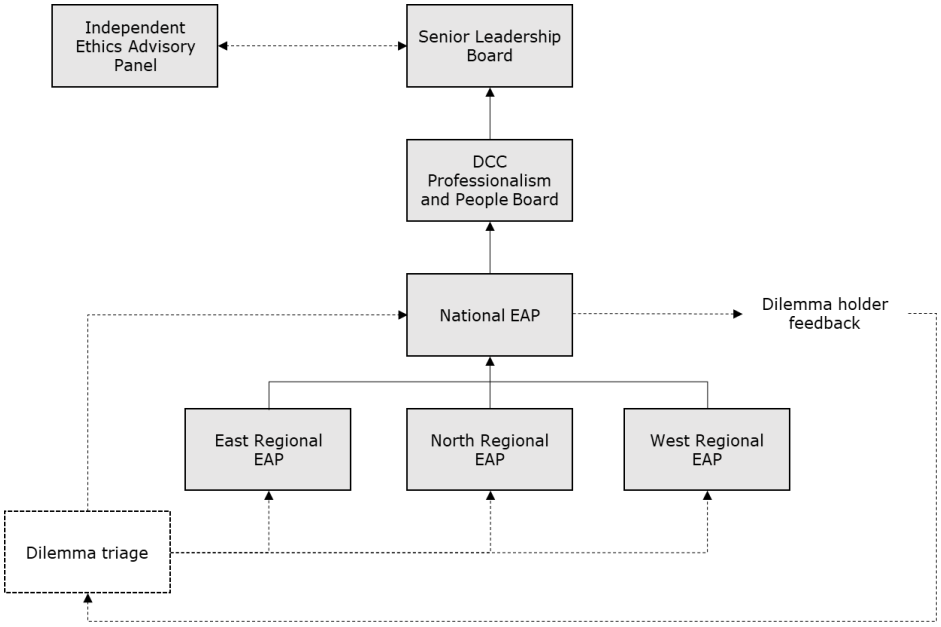

Diagram outlining different ethics processes in Police Scotland

Ethics advisory panels in Police Scotland: A view from Marion Oswald

It would be useful to link this framework to the administrative/committee arrangements that are being established to 'operationalise' this framework - otherwise, there will be a risk that it will principles on paper, but without any oversight processes to ensure that the framework is implemented.

This structure is quite different to the West Midlands PCC (Terms of Reference) and Police Data ethics Committee which was established to oversee technological developments, and has specific terms of reference detailing its aims, principles against which projects will be reviewed, transparency, independence etc.

I believe this structure is generally regarded as best practice in the absence of any nationally agreed model because of its semi-independence and the commitment of the force to the model. However, there are still many issues with this sort of oversight, including the relationship with legal compliance and practical issues around budget and resourcing - 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 Data Ethics Model. The big question that I

would have around the current Police Scotland ethics panels is whether there have the expertise and independence to influence technological developments within the force.

Data ethics in Police Scotland - A view from Police Scotland

Governance that allows reflection and research ahead of continuous service improvement is important to the decision of what technology to implement and how to achieve it in a compliant manner that adds value to the service as a whole. For that reason, CDO works closely with the PS Strategy and Innovation team to undertake early discussions on potential technologies and identify early challenges, which can include the legal basis and provides advice on the work that would be required if there was a decision to consider certain technologies.

A new Data Ethics Framework is being introduced to ensure that any 'data-driven technology' solutions are using data responsibly, and any associated data ethics risks are identified, managed, scrutinised (internally and externally) appropriately. The Data Ethics Framework has been developed in conjunction with the Centre for Data Ethics & Innovations (CDEI). Internal Police Scotland approval has been gained, and we are currently in early stages of the implementation plan, which includes wider socialisation initially with the Scottish Police Authority, and the Scottish Government, thereafter.

A new Digital and Data Design Authority proposal is also current in development, which will ensure that solution designs receive the appropriate level of initial direction setting and guidance from subject matter experts, and also provide a technical review process to formally assess a solution design against agreed architecture standards.

Police Scotland acknowledges that with such a new post of Data Ethics, there is more work to be undertaken to align and integrate the Ethics assessments effectively and with value into the overall decision on determining the legal basis and compliance with legislation. Data cannot be used responsibly or fairly if it is used without a legal basis and vice-versa.

The Data Ethics framework is at an early stage of its development, and from the review comments, it looks like there is some confusion over the difference between the existing Independent Ethics Advisory Panels, and the new proposed Data Ethics governance framework. The new Data Ethics proposals include an additional Independent Data Ethics Group, which follows a similar pattern established by West Midlands Police.

In simplistic terms, the existing Independent Ethics Advisory Panels address the "should we …" type of individual ethical dilemmas.
The proposed Independent Data Ethics Group will focus on the 'how do we …..' implement new data-driven technologies, typically reviewing project proposals.

So, both should be complementary to each other.

Data ethics governance framework proposal by Police Scotland: A view from Marion Oswald

Much thought has clearly gone into this document and I can see that a version of the guidance/triage process developed alongside the CDEI is included. A triage process in order to identify the most high risk applications is certainly a good idea in order to focus effort.

While data is certainly an 'asset', this phraseology may seem odd in a policing document, as it tends to reflect the corporate/commercial way of looking at data. It might be better rather to consider data as one of the fundamentals of fulfilling the policing task – i.e. without accurate data, it is not possible to make legitimate decisions and opportunities to protect the public might be missed.

The document should not only talk about bias etc, but highlight that data and outputs of data-driven technology must not be wrong or misleading, and must not lead to detrimental unintended consequences i.e. these tools must work in the policing context. This means that evaluation methods must be long-term and robust, and that outputs of data analytics should often be regarded as 'intelligence' i.e. with a level of uncertainty attached.

I see also that no decision has yet been made on the structure of any independent oversight committee, and a number of factors for consideration are laid out. While I appreciate the concerns around full transparency, I think these are rather overstated in the document. *Not* publishing the papers, minutes and advice of such a group is likely to have more significant reputational issues for Police Scotland than publishing minutes with appropriate redactions for any sensitive matters. In addition, the need for appropriate secretariat support for such a body should not be underestimated, and this will have some budget implications.

Summary of section

3.14 The general notion of ethics is challenging to operationalise – and in the domain of policing it can be particularly difficult or contentious. However, the ethics associated with emerging technology in policing can be found to be brought into practical terms through the use of impact assessments (understood to be 'live documents' able to adapt to new knowledge), as already implemented by Police

Scotland, and through advisory engagement or debate on proposed initiatives through the organisational practise of consultation and panels/forums. Taking more ethical approaches reflects Police Scotland's lessons learned from past experience, and may improve social acceptance of their technology- relevant practices.
Force policies, guidance, and training are also able to inform officers and staff about ethical standards and the methods in which behaviour is compliant with bias mitigating efforts. Ethical considerations around emergent technology in police work can relate to ensuring and communicating the legal basis for police use of a technology, but also typically consider how technology reifies or augments power relations. Examples of this could include technology enabled mass surveillance or social sorting, expansion of use cases of technology (i.e. function creep), potential chilling effect on populations, collateral intrusion, and insufficient safeguards surrounding analytical capabilities. Police Scotland has many governance processes in place to address the ethical issues discussed in this section, in order to best serve and protect the communities of Scotland from harm. It will be crucial that independent oversight of these ethics processes and due transparency over them are guaranteed and implemented in order to ensure ethical outcomes.

4. Procedures & evidence gathering

4.1 Policing procedures and evidence gathering present legal and ethical issues, which we explore here. In particular, we consider issues surrounding digital evidence, looking at the procedures which should be followed in order to ensure that best digital evidence is gathered and fed into the criminal justice process right through to trial.

4.2 Some commentators consider that there are gaps in the case law of Scottish and English courts in dealing with the expanded scale and scope of interference with Article 8 of the ECHR (respect for private and family life, home and correspondence). Smartphones, the devices being examined by police, are incomparable to paper documents and more basic computers. They store, transmit, communicate and identify data in large amounts, often without the users' control or informed consent. They also often contain jointly owned data or data belonging to others that can be obtained without their consent. For example, a device that identifies locations often cross-references location information with other users in order to determine directions or details about the location. This information may be collected from people who do not and/or cannot consent to its use. Such a conundrum would behave been impossible prior to the advent of smartphones; now it is routine. The information found on a device may provide profound insights into an individual's behaviour, beliefs, and emotional state. Evidence extracted from a digital device may be critical to a criminal investigation, however, not all devices require to be reviewed and they should not be seized and examined as a matter of routine.

4.3 In relation to a criminal investigation, a device should only be reviewed, and information extracted, where it represents a reasonable line of enquiry. What constitutes a reasonable line of enquiry will depend on the facts and circumstances of each case and the changing context of an ongoing investigation. What is also an issue is the technology used to extract this information including bypassing security protocols and analysing metadata. In the Fearon case in Canada, where the prosecutor refused to disclose their methodology to overcome encryption software, and made an application for public interest immunity. When considering these applications, the court must apply a balancing exercise to determine the interests of the defendant in receiving all the information relevant to their defence with the interest of the state in protecting sensitive information. The court in that instance deemed there to be a high level of public interest in allowing the prosecutor to withhold their methodology, as doing so did not preclude a fair trial taking place. This was a case in which the position of the accused was one of disowning the e-mails entirely. The prosecutor accepted that there had been a risk of corruption or destruction of the data in their exercise and there was a discrepancy in their analysis of the numbers of e-mails. Had the defence been of a different nature then there was a possibility that a fair trial would not have been possible. This would have had a considerable impact on the interests of relevant victims. There is a real danger of this sort of capability continuing to exist without scrutiny where a piecemeal approach to regulation is taken.

4.4 When a technology such as cyber kiosks is looked at through the lens of the rationale in the *Marper* case, it is apparent why there is widespread concern. In *Marper* the court remarked about the abundant unique and personal data within a DNA sample that police considered themselves entitled to retain and interrogate without limitation. The fair balance of private and public interest was not achieved by the UK policy given its indefinite nature and the lack of scrutiny applicable to the decision-making process to retain the data. The parallels with cyber kiosks are plainly evident. The finding of the High Court in the aforementioned *Bridges* case on facial recognition that the question of legality was simple and binary contrasts sharply with the holistic approach taken by the Court of Appeal in *Marper*. The court clarified that clear guidance on the use of the technology and who could be targeted were issues of legality and, in the absence of such guidance, a finding that the interference was in accordance with the law was not sound. Further the DPIA was inadequate because it assumed legality without recognising that it was required to assess the rights and freedoms of data subjects and address them accordingly. The Court also agreed that the PSED had been breached because the police did not investigate the possibility of bias on the grounds of ethnicity (race) or gender.

4.5 As mentioned earlier, Scotland is set to become a forerunner in the regulation of biometric data use by police. The SBC draft Code of Practice, once assented by the Scottish Parliament, will become the first of its kind and Scotland will become the first UK country to have detailed legislation, and a statutory Code of Practice on the acquisition, retention, use and destruction of biometric data for criminal justice and police purposes.

Summary of section

4.6 Digital evidence gathering via and from new technologies remains a challenging subject, especially as regards compliance with human rights and equalities objectives. The implementation of the biometrics code of practice in Scotland is a positive step, and this implementation and its evaluation should inform further how procedures and evidence gathering can be improved further to reflect best practice in human rights, equalities and data protection.

5. Lessons learned & good practices

5.1 This section looks at the lessons that can be learned from previous attempts by Police Scotland to adopt new technologies from a legal and ethical standpoint to inform future decision-making and operational use of technology.

5.2 From an organisational perspective, knowledge is typically generated before technology is deployed in the form of Business Cases, Appraisals and Impact Assessments (all of which are assumed to be written, engaged upon and reviewed prior to procurement and deployment). Throughout live change processes or trials, documentation is written and retained to contribute to a post-implementation approach to knowledge production – where the 'lessons learned' can often be found. Once a project has reached completion and becomes part of Business As Usual, many documents are often produced to review and assess the implementation of the change.

5.3 Four case studies from a Scottish perspective are considered: cyber kiosks, mobile working, body worn video, and drones. Through the corroboration of multiple pieces of documentation associated with past implementation of technologies, this section culminates in a discussion about lessons learned from an ethical and legal perspective, taking account of international and comparative developments in this area which may be useful to inform the Scottish perspective.

Cyber kiosks

5.4 In 2016, Police Scotland conducted a trial utilising a digital forensic technology product known as Digital Triage Devices, also referred to as Cyber Kiosks. Cellebrite's Cyber Kiosk technology allows frontline investigating officers to bypass security protections and passwords in order to access data held on an individual's mobile device (like a mobile phone or tablet) seized under a warrant. Cyber kiosks are able to search through SMS and internet messages, images and other forms of media, SIM contacts, and other data held on a personal device allowing lines of enquiry to be progressed quicker. No data is held or stored on the cyber kiosk systems – they are only able to 'triage' or visibly search through devices. Police Scotland have a process in place whereby only trained officers are able to use the devices after a 2-step approval process. It also again must be emphasised that no data is retained on the kiosks, instead they are used to scope contents to determine if any data is held which is of evidential value.

5.5 Prior to Police Scotland procuring the kiosks, a formal business case was not written. As a result, impact assessments were not carried out, stakeholder engagement or public consultation was not conducted, and assurance or oversight mechanisms had not been organised. The primary driver for change identified from the outset was the opportunity for the police to be able to quickly return devices to victims in order to encourage victim and witness engagement.

5.6 It had been previously identified that there were issues associated with long term denial of access to personal devices during investigations which consequently discouraged co-operation from witness and victims.

5.7 Further benefits to using the cyber kiosks were also acknowledged, ranging from:

a) reduced intrusion of individual privacy,
b) early identification of evidence,
c) fewer devices being submitted to Cybercrime Units (improved efficiency),
d) Criminal Justice partners receive a faster and improved quality of service with regard evidential requests (increased effectiveness),
e) Furthermore, they are understood to be resource saving (since less data processing and storage is required, resulting in less transfer implications and associated costs).

5.8 These benefits can be understood and appreciated to be acting in the public interest. However, without relevant legal frameworks which have been consulted upon and ethical issues associated with the technology's introduction having been rigorously accounted for, any initiative which reshapes the dynamic of police work and police powers (such as the cyber kiosk project) may be perceived as problematic by stakeholders and the wider public.

5.9 Whilst the implementation of the Cyber Kiosk project was in a state of limbo from 2018-2020, the Scottish Parliament's Justice Sub-Committee on Policing held an inquiry in order to determine the legal basis for this technology. Open Rights Group, Privacy International, and the Scottish Human Rights Commission were among many stakeholders who believed there was a lack of a clear legal basis for the use of cyber kiosks by Police Scotland. The Scottish Human Rights Commission noted that cyber kiosks have "the potential to be highly intrusive of [the right to privacy, and therefore wanted] to see clear rules and safeguards in place to regulate the use of this technology, and to guarantee robust and independent oversight" (SHRC, 2019).

5.10 Although data retention issues can be understood to be mitigated with the above processes, when thinking about scoping and viewing the contents of an individual's mobile device, there are many ethical and legal contentions that arise. From an ethical standpoint, there is the potential for *collateral intrusion* to occur (defined as intrusion into private life of friends, family, and other people situated in the social network of the individual). Additionally, there is the potential for *police overreach* (if not targeted searches of personal data may be viewed and invasive levels of privacy interference may occur).

5.11 In the ICO's investigation report *Mobile phone data extraction by police in Scotland,* Police Scotland's level of compliance was assessed in relation to the data processing principles outlined in Part 3 of the DPA 2018 which apply to the processing of personal data for law enforcement purposes. The findings of the report found some inconsistencies in relation to meeting the six principles that apply to personal data processing for law enforcement purposes, and more generally made recommendations when considering mobile phone extraction in Scotland.

5.12 The report includes a number of recommendations for Police Scotland including: the reviewing and updating of Data Protection Impact Assessments (DPIA); consultation with the ICO when any new, high risk processing of data is proposed; implementation and maintenance of the ISO/IEC17025 certification standards; the revision of privacy information documents supplied to the public, and the revision of internal policy data management respectively.

5.13 These recommendations should also be considered as opportunities for lessons to be learned as a result of the Cyber Kiosks project – but these recommendations can also be extrapolated when thinking about any future implementation of new and emerging technology. Had the ICO been consulted or a DPIA been conducted prior to the Cyber Kiosks deployment, legal issues may have been identified and mitigated against prior to parliamentary action taking place.

5.14 Police Scotland produced an End of Project Report (EPR) for Cyber Kiosks in April 2021. The report recognised that there was not full consideration or consultation towards relevant stakeholders concerns in relation to the use of cyber kiosks. The force note that the technology was already being used in different areas of the service (i.e. cybercrime hubs), however Police Scotland subsequently recognise they did not anticipate or spend enough time considering public concern or perceptions regarding the new use of the technology.

5.15 Within this commendable self-recognised misjudgement, it can be observed that there is a lesson to be learned in that *public consent and public concern was not identified or anticipated adequately enough*. An effective risk management approach attuned to external publics and effected groups may have mapped and spotted this issue. Ultimately, public discontent with police use of technology can become an ethical risk due to communities who are alarmed or apprehensive about the potential misuse or intrusive processing of data and/or unnecessary retention (which contributes to a legal data protection implication also). Negative sentiment or perceptions may potentially lead to loss of confidence in policing and the exacerbation of misunderstandings about police policies or practices. Furthermore, the *lack of a formal business case* being produced meant other mitigation assurances (*such as impact assessments or governance/assurance structures*) and *lack of engagement (or consultation)* can all be considered areas where there are lessons to be learned. Going forward, *any proposed technology procurement project must follow the HM Treasury Green Book's business case framework*.

5.16 Reasonable consideration was not paid to the notion that that there was a reshaping of police powers by virtue of the cyber kiosk technology's adoption. Previously the kind of forensic technological capability cyber kiosks enabled was only in use in Cyber Crime hubs in Scotland, with accredited digital forensic practitioners able to utilise such technology. This gave rise to critical consideration towards the legality of the cyber kiosks' use and legal basis for their deployment being questioned. Furthermore the cyber kiosk initiative highlighted the need for police organisations to be able to communicate to the public what a technology or novel practice entails, informing the communities that a force serves with objective information detailing any new capabilities.

5.17 The Justice-Sub Committee on Policing inquiry found that Police Scotland used the cyber kiosks to "search the mobile phones of suspects, witnesses and victims of crimes […] without undertaking the required governance, scrutiny, and impact assessments" (SPJSoP, 2019: 12). From a legal perspective, Police Scotland had been treating mobile devices as they would physical property in terms of their seizure and examination procedures – however laws relating to physical property fail to account for the unprecedented scope and granular quality of potentially intimate personal data and information which can exist on an individual's personal device.

5.18 In the Conclusion of the Scottish Parliament Justice Sub-Committee on Policing Report *Police Scotland's use of remote piloted aircraft systems and body worn cameras*, the following is found:

> The previous inquiries undertaken by the Sub-Committee into Police Scotland's plans to introduce digital device triage systems and facial recognition technology, demonstrates the risks involved in introducing new technologies to policing. It confirmed the need for necessary assessments to be undertaken, the legal basis for the use of such technologies to be confirmed, and relevant stakeholders to be consulted prior to a decision being made.

5.19 While Cyber Kiosks are an example of such measures not being well implemented and followed, Police Scotland assert that it has learned lessons from the Cyber Kiosks scenario in how to go about implementing policing technologies in appropriate ways from a societal perspective. Various tools are used by Police Scotland to achieve this, including post implementation reviews and external evaluations.

Lessons learned & good practices: A view from Police Scotland

Post implementation reviews

Police Scotland utilise a Post Implementation Review (PIR) process. A PIR is a formal review of a project and part of Police Scotland's project assurance framework. It is used to answer the question, "did we [Police Scotland] achieve what we set out to do in business terms and if not, what should be done?" In relation to Police Scotland's roll out of Cyber Kiosks in 2021, it issued an Update paper in June 2021 which identified some of the key findings (similar to the External Debrief). The themes identified in the update paper as part of the PIR were: Governance, Teamwork, and External Consultation.

Governance

The lack of governance at the outset resulted in many key challenges and obstacles that required to be addressed before the project could progress. It is understood

within Police Scotland, that had a Business Case, Equality, Human Rights Impact Assessment (EqHRIA) and a Data Protection Impact Assessment (DPIA) been completed in advance, the project would have had a greater understanding and would have been more fully equipped to address the challenges that subsequently ensued. The procurement exercise was carried out by Operational Policing, however the required consultation did not commence until after the purchase of the Kiosks. This is now something that would be managed within the Transformation Portfolio and forms part of project governance guidelines.

Teamwork

The review team noted that working relationships between the external stakeholders and the project team was challenging to begin with. This was due to a number of misconceptions surrounding the proposed use of Kiosks. The team worked hard to build confidence and relationships, improving rapport between the internal and external focus groups over time, which did not come without its challenges.

External consultation

The review team also noted that failure to consult with a wide range of external stakeholders and reference groups from the outset led to a lengthy engagement and debate process including an investigation into the use of Kiosks by the Scottish Parliament Justice Sub Committee. During this time a wide range of concerned bodies were heard on issues relating to introduction of Kiosks and a total of five evidence sessions were held. This lack of consultation resulted in a lengthy delay in the rollout of Kiosks. These key learnings relating to police use of technology and data, and the key requirement for consultation have been captured in the Lessons Learned exercise undertaken by the project team and documented within the EPR. There are lessons learned to be observed surrounding:

- Legal assessment
- DPIA
- EqHRIA
- Engagement with stakeholders
- Consultation
- The need for clear safeguards being a requirement.

Mobile working devices

5.20 Starting in summer 2019, a roll out of Mobile Devices to community and response officers was initiated as part of the Mobile Working Project (Phase 1). This project saw the deployment of 10,809 mobile devices and a suite of associated policing applications to operational officers. The Mobile Working Project is a part of the larger ‘Digitally Enabled Policing Programme’ (DEPP), and aimed to equip officers with a digital mobile policing device to replace the outdated paper notebook system. Increasing efficiency, it was also slated to provide remote, live access to key policing information systems.

5.21 A research team from Robert Gordon University (RGU) and Abertay University were appointed to evaluate the implementation and impact of the national roll-out, and to inform the final stages of roll-out to 10,000 police officers across Scotland. The findings of the research were largely positive. The research team were able to identify long-term potential benefits in five main areas with a number of sub-themes as highlighted below:

- *Productivity* - Efficiency, Increased capacity, Proactive policing, Time management, Time saving.
- *Information* - Access to information, Information accuracy, Immediacy of information, Additional information sources, Information sharing, Security of information.
- *Connectivity and Communication* – Connectivity, Real time communication, Team Communication, External communication, Increased visibility.
- *Officer wellbeing and safety* – Officer wellbeing, officer morale, officer safety, autonomy, Covid-19.
- *Technology and Culture change* – Officers attitudes to technology, Members of public attitude to technology, Culture change, Logistics, New working practices, Collaboration, Improved relationships.

5.22 There were also a number of recommendations reached as a result of the research, to complement the realisation of the benefits identified. These recommendations can act as an indicator at areas for future learning as an example of a largely positive and frictionless attempt to implement new technology.

5.23 Recommendations

Training - Generally positive comments about practical training session, less positive about Moodle training: a blended approach was identified to be ideal in the future;
Engagement with officers in device development - Officers are interested in identifying ways to improve the device, and have been using the 'feedback function' to do so (user feedback);
Timeline for requested additional functions communicated – User suggestions for functions that would be helpful, e.g. VPD. Keeping officers informed of developments may encourage continued engagement;
Need for a strategy for maintenance and replacement of devices with financial and organisational backing. There was concern expressed about the sustainability of the devices as technology improved;
Interoperability of systems - While many interviewed highlighted the collaboration and better information sharing that the devices allowed, some commented that this needs to be increased;

All processes and governance with the new ways of working be reviewed regularly to create timely new systems - There was a realisation that the existing procedures based on the traditional notebook system might need some review and that might need to be ongoing.

5.24 In comparison to the Cyber Kiosk project, the Mobile Working project suffered relatively low levels of contention and resistance. This could be attributed to the fact that the technologies are relatively non-intrusive and do not directly interfere with the rights or impact upon citizens directly. A formal business case was written for both phases of the project, and subsequent impact assessments and engagement had been carried out. The mobile working devices' main benefits relate to their ability to expedite outmoded processes – i.e. to increase efficiency and effectiveness. As such, there were limited legal or ethical concerns in which lessons could be learned apart from the aspects of the project related to data security (covered in Police Scotland's data protection impact assessment); or the proficiencies offered to frontline officers (e.g. which saw increased communication benefits). However, both of these legal and ethical concerns associated with the mobile working technologies can be understood to contribute to *positive legal and ethical impacts*: e.g. owing to the strengthening of data security, increased access to information and more efficient communication which contributes to a more effective delivery of justice.

Drones (RPAS)

5.25 The use of remote pilot aircraft systems (RPAS), otherwise known as drones, by police, commercial organisations and individuals has increased hugely over the course of the last decade. NESTA reported that in 2010, there were five commercial permissions for drone operation and, by 2018, there were 4,530. Drone registration was extended in 2019, with all drones above 250g in weight or equipped with a video camera, whether operated by commercial or individual users, with around 200,000 registrations as of March 2021. Despite this huge increase, research suggests that there is some public concern around the use of drones, not just for policing but more generally.

5.26 Drones are now used by police forces across the UK, including in Scotland, and in a range of different types of activity, from surveillance to assisting in finding missing persons or road traffic incidents. The technological capability of drones raises legal and ethical issues that need to be considered in their deployment. As an emerging technology, drones are capable of viewing people from vantage points in which there might otherwise be an expectation of privacy, at distances where there may be limited appreciation that drones are in operation, with infrared or low light capability, and potentially using automatic number plate recognition or facial recognition technologies.

5.27 Drones engage some specific issues as an emerging technology and also share issues in common with other emerging technologies, such as facial

recognition; though it is noted that the Police Scotland fleet does not currently have facial recognition capacity, nor is there any current intention to include this. In considering deployment of drones in a policing context, it is important to recognise the different contexts in which drones may be deployed. Legal issues, such as the right to privacy may engage to very different degrees depending on the deployment context, for instance, between supporting a search for a missing person in a rural area to surveillance at a large scale public event.

5.28 The use of drones is subject to a number of legal requirements, including compliance with human rights and data protection requirements, equality requirements, and Civil Aviation authority regulations. The need for robust impact assessments is critical. As drones will likely capture sensitive personal data – likely to be gender and race at least - there is a requirement to demonstrate that no less intrusive means are suitable. For drones, the risk of 'collateral intrusion' may be more extensive than for other means and demonstrating this necessity will be an important element of any impact assessment process. One of the categories that constitute sensitive personal data is political belief so deployment, for instance, at a public protest would require detailed justification.

5.29 There is detailed guidance from the ICO on the use of drones. Measures required may include the prohibition of continuous recording, restriction of recording at lower altitudes, restricted field of vision or other means. One particular challenge may be the requirement to provide notification of drone operation in an area. It may be easier to deploy signage for a drone deployment to assist with a traffic incident than for a missing persons search over a wide geographic area. Privacy by design is required, and this will include the development of specifications for police drones and their procurement. For example, any data stored locally on a drone should be encrypted, in the event that the drone should crash and be retrieved by a third party.

5.30 Though the use of drones has not seen significant challenge in courts in Scotland, because of the commonality of the legal framework across the UK, court decisions elsewhere have considered similar issues. For instance, in the aforementioned *Bridges* case in England and Wales, the legality of drone deployment at public events was considered, although the case was about live facial recognition use.

5.31 Internationally, the use of drones in a policing context is still at an early stage. Some jurisdictions have considered the legality of the use of drones under prior legal frameworks, testing the legality of drones on the basis of prior frameworks around police helicopter surveillance, intentional interception of oral communications, or the 'extra-human' capability of police canine deployments. A number of states in the US have prohibited the use of drones for police or other surveillance on constitutional grounds, including Florida and Texas, though in the latter a judgment upheld the legality of drone surveillance by investigative journalists as a protection of the First Amendment right to freedom of speech.

Body worn video

5.32 The Lady Elish Angiolini Independent Review into complaints handling, investigation and misconduct issues, published on 11 November 2020, recommended that Police Scotland should accelerate its plans to expand the use of body worn video (BWV) technology. Furthermore, in January 2021, Chief Constable Iain Livingstone stated that there was a “pressing, critical, ethical and operational imperative" to ensure armed officers were equipped with the devices in time for COP26 in November 2021. Armed policing is an area of high risk and understandably high public scrutiny, therefore the business case outlining the requirement to invest in BWV technology was presented to the Board of the Scottish Police Authority during the June 2021 Authority meeting.

5.33 BWV is understood to provide several benefits for armed police officers given the specialist and potentially life-critical nature of their work. BWV increases the transparency of policing as any footage recorded can be subsequently reviewed, scrutinised and submitted as evidence, making officers as well as offenders, more accountable. A major advantage of BWV is the provision of increased evidential quality. Traditionally, a police officer will make a written record of an incident (including language and gestures that were used) as soon as possible after the incident occurs. When BWV is used, the incident is recorded in real time, limited by the field of view and audio range of the device. This evidence is deemed to be more accurate and detailed than was previously possible.

5.34 BWV footage has similarly been used to resolve complaints made against police officers by members of the public. This reduces investigative time and provides an accurate record of the situation. There is also evidence to suggest that the conduct and behaviour of both the public and officers is improved when BWV is in use. When all parties are aware that they are being surveilled, evidence suggests anti-social behaviour is reduced and the subjects involved internalise an external value system – signalling that they may consider the perception of their actions and conduct more closely.

5.35 Whilst there are many potential benefits which could provide a positive ethical impacts, there are also associated risks with police use of BWV if the technology is not subject to sufficient governance, oversight, or ethical consideration. For example, non-profit international digital rights group Electronic Frontier Foundation outline potential threats such as:

- The capturing of audio and visual data/footage of victims of domestic violence or sexual assault; of children or people suffering trauma-related distress;
- The requirement to safeguard vulnerable individuals from being recorded without their informed consent;
- The potential systematic surveillance of people engaging in the right to freedom of assembly or freedom of association - with subsequent chilling effect on those communities;
- Issues associated with editing or deletion of footage; or with officer discretion deciding when and what to record.

5.36 BWV has been used a limited extent by Police Scotland, primarily in the North East of the country used since June 2010. This began with a pilot for the use of BWV in a designated area within legacy Grampian Police. The pilot showed that BWV offered significant organisational benefits ranging from evidence gathering, enhanced prosecution evidence, and for use in the event of a complaint against the police. This resulted in greater uptake of BWV device use across the region.

5.37 Police Scotland rolled out BWV to armed police officers prior to the COP26 conference in Glasgow in November 2021. Armed policing is a particularly high risk area of policing; scrutiny and the roll out of BWV is thought to help improve transparency and accountability.

5.38 From a legal perspective, BWV devices have the potential to provide the Crown Office and Procurator Fiscal Service with high quality evidence to support investigations and prosecutions. Furthermore, they support investigations by Police Scotland and the Police Investigations and Review Commissioner (PIRC) in respect of investigations concerning the policing response to a particular matter.

5.39 There are recognised privacy, data and policy concerns. To anticipate and mitigate against potential privacy and third-party concerns, Police Scotland completed a full Equalities and Human Rights Impact Assessment (EqHRIA), and Data Protection Impact Assessment (DPIA). These impact assessments are treated as live documents and therefore reviewed or updated annually to reflect changes in legislation, policy and technology. Police Scotland have also developed and published a detailed Code of Practice which outlines how BWV will be used by armed policing.

5.40 Furthermore, on 3 February 2021 Police Scotland launched a survey engaging with the public to obtain their views on the Use of BWV. The purpose of the 3 week survey was to help inform the deployment of BWV for armed response officers across Scotland, capturing the views of 8,835 respondents. Overall, Police Scotland report that there is widespread support for the use of BWV (90% of respondents felt that Body Worn Video should be worn “often” or “always”); with BWV having the potential to increase trust and confidence in Police Scotland (78% of respondents reported that BWV would increase their trust in Police Scotland, and 72% of respondents reported that BWV would make them feel “much safer”).

Body worn cameras pilot – A view from Police Scotland

In June 2010 legacy Grampian Police, now North East (NE) Division, Police Scotland carried out a pilot programme using body worn video cameras. The following information is drawn from the trial of the BWV technology. The evaluation work was overseen by a Project Board, made up of senior staff from legacy Strathclyde Police, Grampian Police and the Crown Office and Procurator Fiscal Service. A Project

Team, including operational staff from each of these organisations and from Renfrewshire Council, led in the evidence gathering to support the evaluation.

A Data Protection Impact Assessment (DPIA) was completed and approved for the use of BWV within NE Division. It acknowledged that BWV would capture personal data visual and audio formats and identified how that data would be stored and managed. The BWV devices and back office systems have end-to-end encryption and footage is automatically deleted from the devices upon docking and being successfully uploaded to the main server. Recorded footage is the responsibility of all trained users as designated through Role Based Access Control (RBAC). Footage that is not required for evidential purposes is automatically deleted after a specified period of time, currently set at 31 days. Evidential footage is marked by the officer for retention and then stored on a secure server. The retention of this footage is then subject to the Police Scotland data retention policy.

NE Division completed an Equality and Human Rights Impact assessment (EqHRIA) and included reference in the Guidance Document that officers should be cognisant at all times of the impact that the use of BWV could have on an individual's Human Rights.
As part of the North-East evaluation, a number of lessons are identified from a public interest perspective. This research noted:

Lessons learned

- Vulnerable individuals may have already have negative experiences of the Police or other public services. How can we ensure that BWV builds the trust of these individuals?
- How do we communicate how BWV will be used and reduce the public's concerns about privacy and GDPR?
- How should BWV be used in sensitive situations or with vulnerable individuals, if at all?
- How do we balance an individual's right to privacy and permission with officer and public safety?

In terms of the lessons learned from the trial implementation of BWV technology, most of the ethical and legal considerations arise from concerns associated with citizen's rights and communication endeavours to promote trust. Scrutiny of proposed procedures and engagement with relevant stakeholders would attribute itself to consolidating many of the identified ethical and legal issues. Transparently publishing documentation including Standard Operating Procedure (SOP), Code of Practice (CoP), Data Protection Impact Assessment (DPIA) and Equality and Human Rights Impact Assessment (EQHRIA) would probably be beneficial. Furthermore this would generate democratic discussion and engagement in order to ascertain social acceptability of proposed future implementations of new technologies.

Insights from other jurisdictions

5.41 The Call for Evidence responses generally compared Scotland to England and Wales in terms of policing, technology and legal frameworks. There were examples of highly localised initiatives within justice from areas of the United States and Canada. The Fractals submission contained a number of links to literature relating to global practices. Ethics review panels were highlighted as a feature of NZ and England and Wales frameworks. The UK processes for data sharing are of particular importance as they incorporate and interact with Scottish databases in a number of areas albeit within different ethical and legal frameworks.

Canada

5.42 Equivalence has been drawn in this context between Art 8 ECHR and, in Canadian domestic law, section 8 of the Charter of rights and freedoms which provides that everyone has the right to be secure against unreasonable search and seizure.

5.43 The Canadian Supreme Court has developed a growing body of jurisprudence distinguishing between traditional searches of physical spaces and searches of devices and cyber space. The case of R v Vu was cited in the legal advice to Police Scotland on the legal basis for Cyber kiosks including the following paragraph (R v Vu 2013 SCC 32 at 45):

> *'These numerous and striking differences between computers and traditional "receptacles" call for distinctive treatment under s. 8 of the Charter. The animating assumption of the traditional rule — that if the search of a place is justified, so is the search of receptacles found within it — simply cannot apply with respect to computer searches…'*

5.44 The superior case of Fearon determined that a search of a mobile phone was not "inevitable a breach of privacy". Fearon is a useful discussion point as it was decided on a 4-3 majority with a strong dissenting opinion provided. Both opinions agreed on the basis set out in Vu that searches of digital devices were distinguished from searches on premises and engaged a potential for far greater intrusion. Both agreed that the potential value for law enforcement of a search of a digital device was very useful. Where Judge Cromwell led was in determining that privacy safeguards could be arrived upon that would preserve the human rights of the target of the search

> "In his view, three such modifications would do this:
> *The scope of the search must be tailored for the purpose for which it may be lawfully conducted. That is, the "nature and extent" of the search must be truly incidental to the particular arrest for the particular offence. In practice, this will mean that, generally, only recently sent or drafted emails, texts, and photos, and the call log may be searched. However, this is not a hard and fast rule – the test is whether the nature and extent of the search are tailored to the search's purpose.*

The discovery of evidence purpose for a search incidental to arrest must be treated restrictively. That is, a warrantless search can only be performed for the discovery of evidence when the "investigation will be stymied or significantly hampered" if the cell phone cannot be promptly searched.

Officers must make detailed notes of what they have examined on the phone. Justice Cromwell frames this as a "constitutional imperative," and writes that record keeping will facilitate after-the-fact judicial review and have the officers focus on the question of whether their conduct falls within their common law powers."

5.45 There are compelling parallels here. The decision to search a digital device here is to some degree subjective. Officers would require precise and detailed legal training in order to balance the necessity of performing a search against the rights of the individual in a proportionate manner. Following the logic of Bridges, the legality does not simply arise out of the fact of being an officer making an arrest. The officer deciding to search must be capable of comprehensively appreciating the human rights being engaged at the time. This includes an appreciation of the criteria of the person being targeted by the search. Any issues affecting accessibility of the law in this instance may reduce the legal certainty that is required under the rule of law.

5.46 There is some controversy about the clarity and ambiguity or lack thereof in the legal opinion obtained by Police Scotland which discussed these Canadian cases. Its author cited these Canadian cases explaining the complexity of the decisions to be made, but contained limited analysis of Article 8. The author points out that the common law authority on this in Scotland is dated, possibly only because it has not been challenged by an appropriate case that might revise it in a modern context. It should be borne in mind that Fearon is a 2014 Canadian case and the advance of technology has greatly increased the capabilities of both digital devices and those who would intrude upon them since then. The author made several recommendations and identified legislation and a code of practice as best practice. Asserting that the opinion was clear and unambiguous was to obscure the context of the advice and interpret it in as narrow a way as possible. It is concerning that Police Scotland considered the issue to be satisfactorily resolved without attending to these recommendations.

5.47 Considerable discussion in Canada has also taken place regarding emerging technologies and policing revolving around the use of algorithmic policing and its engagement with Section 9 of the Canadian Charter, the right not to be arbitrarily detailed or imprisoned. This has been tested in the courts finding that where police detain persons based on aggregated data analysed by artificial intelligence, Section 9 is breached as suspicion based on this sort of evidence is not held to be reasonable.

5.48 The Canadian jurisprudence has acknowledged that the profiling of suspects on the basis of their ethnicity is unlawful. In modern terms this extends to any sort of

technology that relies on a data set as there is always potential within the data set to reflect bias(es).

5.49 While Canada has had some of these issues litigated it is clear that there does not yet exist a comprehensive framework covering all aspects of emerging technologies.

New Zealand

5.50 The Privacy Commissioner of New Zealand (a role similar to the UK's Information Commissioner) considers their legal framework to be adequate to address the field of biometric deployments. The principal legal instrument here is the Privacy Act 2020 which recognises the potential harms to individuals caused by breaches of privacy. They consider use of technologies such as facial recognition to fall into this context, although on the limited basis of technology for identification purposes. This can be contrasted with EU GDPR which offers protections for a variety of data use categories. NZ Authorities are considering whether the statute can be supplemented by a code of practice to give this type of effect. The Privacy Act applies to both public and private bodies, an insightful intervention given the interdependent nature of technological advance.

5.51 A feature of NZ immigration legislation is a limit on the use of artificial intelligence in decision-making and a requirement to prescribe personal responsibility to such decisions. Although limited to Immigration, the jurisprudence developed therewith may be persuasively applied across the board. As it happens, the Immigration legislation is the statutory basis for privacy impact assessments recognising the vulnerability of individuals and immigrants

5.52 Many NZ Government agencies have voluntarily subscribed to an Algorithm charter for Aotearoa New Zealand that provides a legal framework for Artificial intelligence related products and services. This shows that even where the law is reticent, NZ agencies actively seek consensus and a framework that provides accountability and transparency. The Privacy Commissioner also has the ability to establish legally binding codes of practice in a manner similar to that of the new Scottish Biometrics Commissioner. There is more of a centralisation of regulatory powers in this area in New Zealand with the Privacy commissioner having two other statutory mechanisms under their supervision in relation to electronic identification, namely Electronic Identity Verification Act 2012 and Identity Information Confirmation Act 2012.

International

5.53 There are well established international norms and international law in play when it comes to law enforcement. A respect for fundamental human rights derived from the ratification of UN treaties incorporates at an advisory level, the work of the UN Committees and the text and commentary on United Nations Treaties. In relation

to the police approach to modern technology we can adapt the approach of distilling key principles from international law sources such as Article 17 ICCPR. This declares a right to privacy and freedom from arbitrary, unnecessary, disproportionate intrusion. Police searches should not be more intrusive than absolutely necessary to achieve their purpose and should not be disproportionate in scope certain types of intrusion such as phone tapping reserved for most serious crimes.

5.54 Another sphere of relevant international law and standards is the Council of Europe and its delegate bodies such as the Committee for the Prevention of Torture. These bodies have established detailed legal frameworks, some of which are binding at law, for policing and in particular the use of modern technology by policing agencies. Finally international non-governmental organisations (NGOs) such as Amnesty International and the International Committee of the Red Cross (ICRC) have published guidance on policing based on their professional functions and research.

5.55 An examination of the international sphere tells us is that Scotland is not unique in finding this area challenging. The problems and discussions have drawn the attention and efforts of an assortment of international bodies, for example the Council of Europe Convention for the Protection of Individuals related to Personal Data, paraphrased in the Biometrics IAG report:

'*the introduction and use of new technologies should take full account of, and not contravene, fundamental principles as the inherent dignity of the individual and the respect for the human body, the rights of the defence and the principle of proportionality in carrying out of criminal justice'*.

5.56 The UN High Commissioner for Human Rights has noted that digital technologies '*threaten to create an intrusive digital environment in which both States and business enterprises are able to conduct surveillance, analyse, predict and even manipulate people's behaviour to an unprecedented degree*', and thus put the right to privacy at serious risk.

5.57 Other international standards that should be given due consideration are the jurisprudence and general comments of human rights bodies to which the UK is a member. UN independent experts have also developed relevant guiding principles concerning the use of personal and non-personal information. The UN Guiding Principles on Business and Human Rights should be also considered. There is a legitimate expectation that private actors (e.g. developing and innovating new technologies, which then may be used by police) should comply with all applicable laws and respect human rights.

5.58 The UN Secretary General has underscored, '[w]e have a collective responsibility to give direction to these technologies so that we maximize benefits and curtail unintended consequences and malicious use'.

Facial recognition internationally

5.59 Facial recognition use by police has attracted significant controversy internationally, with discussions of prohibitions of at least some police uses of it. As mentioned earlier, Scotland has at present adopted a moratorium on police use of live facial recognition technology.

5.60 Feeding into Scotland's decision were the US states and municipalities which have implemented severe restrictions on Facial recognition technology recognising the strong evidence of discrimination associated with its use. Countries such as Morocco have followed suit. Perhaps more interesting though is that In June 2020, Amazon, IBM and Microsoft all stated that they would not sell any facial recognition technology to US police forces, amid increasing concerns about racial injustice in the US and the racial bias that has been found in facial recognition software. While this distancing represents a small proportion of the market in this type of technology it shows that private actors cannot reflect societal concerns without a stringent legal framework being in place.

5.61 It is notable that the European Parliament has supported the European Commission's call for a five year ban on police use of facial recognition and predictive policing algorithms. This is part of an international campaign of concern over the levels of surveillance by states and private actors which the United Nations considers to be incompatible with fundamental human rights. Where individuals have gathered to protest for example, the use of facial recognition can serve to intimidate and deter people from protesting.

5.62 In strong contrast, England and Wales have deployed facial recognition and other technologically based policing methods for a number of years, some in partnership with private organisations. There is no specific legal framework for this type of policing with what little regulation exists being saved for fingerprints and DNA evidence. The *Bridge* case highlighted the need for a legal framework in England and Wales for this type or policing beyond Police common law powers which were found to be inadequate.

AI and the European Union

5.63 While the UK, and therefore Scotland, is no longer an EU Member State or subject to EU law, developments in the EU are of interest from both a comparative and trading perspective. One such development is that of the proposed AI Act, currently making its way through the legislative process in Brussels. The proposed Act, even more so than the GDPR on whose model it is built on, is a domain-neutral proposal that cuts across sectors and the private-public divide. While there are a

number of exceptions, for instance uses by the military, it applies, unlike the GDPR, also to police and other law enforcement actors in the EU.

5.64 The Act lays down harmonised rules for the development, placement on the market and use of AI systems, though with a marked emphasis on the development and placement side at the expense of down-stream use.

5.65 The Act uses a risk-based approach that creates four categories of "risky" systems and their deployment), with a scale of legal constraints from the most severe (always prohibited) to the most permissive (mere encouragement of codes of practice)

5.66 In particular, it distinguishes between systems that pose:
an unacceptable risk and are therefore generally prohibited – though law enforcement enjoys a number of exceptions;

- high risk systems that are permitted but more heavily regulated;
- limited risks systems to which some regulation applies; and
- minimal risks systems that are not regulated, though the development of and adherence to codes of practice and similar frameworks is encouraged.

5.67 Uses of AI by the police potentially cut across all four categories, though it is explicitly referred to under the rules pertaining to a) and b). Given the wide definition of "AI" which includes statistical analysis software, some software used routinely by law enforcement agencies for some time, and without raising particular concerns (or at least not concerns framed in the language of trustworthy AI) could fall under the high-risk category, as no explicit grandfathering provision is in the Act. This may include tools such as automated number plate recognition or forensic DNA matching.

5.68 The EU's AI Act may have relevant implications even for a post-Brexit UK and Scotland. There are three types of implications:

- direct legal issues resulting from the extraterritorial scope of the Act;
- pragmatic, de facto regulatory pressure for UK businesses and law enforcement as result of the Act; and
- the question whether the Act provides a good blueprint for Scotland to follow, even if this is not a requirement.

a) Legal implications

5.69 Just like EU data protection law, the Act has (at least some) extraterritorial reach. It provides safeguards for residents within the EU also against the use of their data by providers of AI services located abroad, which would include organisations in Scotland.

5.70 The obligations under the AI Act are independent of any adequacy findings for EU data protection law purposes. This means that at least in principle, even when data of EU citizens has been transferred lawfully for processing to a third country outside the EU under an adequacy finding of the receiving country's data protection laws under EU data protection law, processing of that data may still fall foul of the

additional requirements that the AI Act creates when this processing involves automated analysis and decision making using an AI as defined by the AI Act.

5.71 This has implications for UK businesses providing AI services that also involve residents of the EU, but it could potentially also affect cross-border police cooperation and data sharing.

b) Pragmatic implications

5.72 It is clear that the EU's aspirations are that just like the GDPR in 2018, the EU AI Act will become a global standard. While it can be doubted whether the two Acts are really sufficiently similar to have similar effects in this regard, the EU proposal is already having some international impact. In late September, Brazil's Congress for instance passed a bill that creates a legal framework for artificial intelligence that closely matches the AI Act. At the same time, the US is also stepping up its efforts to regulate development and use of AI systems.

5.73 UK based developers of AI systems and providers of AI-supported services will have to be mindful of these developments and will often have to work towards compliance with these standards. Care has therefore to be taken that any UK or Scottish initiative in the same space does not needlessly multiply compliance burdens.

c) The AI Act as regulatory blueprint within the UK including Scotland?

5.74 Some of the substantial issues of the Act for the regulation of AI by law enforcement were already discussed above. Here two key structural features of the Act are noted.

5.75 The Act's ultimate aim is to minimise trade barriers for AI products and services within the EU Single Market. This means that it preempts, possibly on a significant scale, the ability of Member States to regulate in response to local conditions, and in particular to impose more demanding rules. If a similar Act were to be adopted by the UK legislature, then similar issues for the ability of the Scottish Government to regulate AI in policing might arise.

5.76 This is related to the broad subject matter of the Act. The Act is conceived as domain independent, and in particular includes policing, unlike the GDPR. However, this aspiration is not really fulfilled, as law enforcement is subject to so many special rules (some more permissive than those for the private sector, some more demanding). The advantage is that this mitigates the problem of demarcation issues between the risk categories. All use of AI by the police, be it in their "investigative" capacity or in their role as employer are covered. Still, within the context of devolution this creates additional issues and questions – presumably a Scottish AI Act can only regulate those uses of AI that are in turn devolved matters, further

diminishing the advantages of a “single” Act. For this reason alone more domain specific approaches that trace devolved powers seems preferable.

5.77 In any event, as mentioned earlier, the current UK-wide approach to AI regulation is to issue a set of non-statutory cross-sectoral principles on AI. This approach may change, as the UK Government is currently soliciting feedback on its proposals, which may alter what happens. It would be advisable for a binding code of practice to be adopted for AI uses by police in Scotland given concerns which have arisen with previous technologies by police in the absence of such a code.

Summary of section

5.78 In Scotland, the main areas in which lessons can be learned relating to the adoption of emerging technology relate to the following 6 considerations: (1) How capabilities are communicated by police (to multiple stakeholders); (2) Engagement and consultation; (3) Governance structures and oversight process; (4) Identified legal basis; (5) Effective and matured risk management processes; and (6) Horizon Scanning.

5.79 How capabilities are communicated by police (to multiple stakeholders) – it is crucial that communication regarding substantial changes to the nature of police work mediated by technology is clear, publicly facing and speaks equitably to a broad range of publics.

5.80 Engagement and consultation – a strong democratic engagement and/or consultation process must be enacted upon in order to gain insights from the communities that a police service works for. In Scotland, if the policing by consent model is to be adhered to, then the public should be involved in changes to the policing system which could change the fabric of society.

5.81 Governance structures and oversight process – this area has seen the most amount of positive work in Scotland, whereby robust structures which allow governance processes to be followed and effective oversight to be attained are now frequent features of new change initiatives in Scotland. Learning from past mistakes has allowed for the Memorandum of Understanding to be built which addresses this area.

5.82 Identified legal basis – some kind of legal basis assessment must be considered before any new technology is implicated in policing to understand the power which comes from what law which sanction the use of a technology (then for example; proportionality and necessity testing; accurate and reliable/scientific standards, EqHRIA and community impact assessments should follow). This must be clearly communicated to stakeholders and the public.

5.83 Effective and matured risk management processes – the continued improvement of a risk management throughout an organisation will be crucial in scoping, mapping, identifying and addressing any risk, opportunity or issue which

may become associated with the adoption of a new technology. With a risk-based approach to understanding contexts and stakeholders, there will be greater emphasis placed on considering social impacts of technology and ways to understand how communities will respond to proposals.

5.84 Horizon Scanning - Elsewhere around the world, there are also lessons to be learned from similar jurisdiction. The methodology to gain insights in this regard is known as horizon scanning, and will continue to be crucial in knowledge exchange, information on best practice, and the consideration of high risk initiatives which may not be acceptable in Scottish society.

6. Looking to a fair future

6.1 Especially since the Cyber Kiosks scenario in 2018-2019, Police Scotland are more mindful of the ways in which Article 6 ECHR (right to a fair trial) is engaged in the carrying out of their functions. However, there may be consequences of police activities with digital technologies that are unintended and unknown, and which may also impact Art 8 (right to private life) and/or have specific impacts for the protected groups in EA 2010. There is limited analysis or evidence of how policing activities may engage Art 8 or EA 2010 provisions when police use new technologies.

6.2 In addition, there are also distinct and emerging risks that widespread use of surveillance tools and AI-enabled technologies is undermining citizens' digital rights and hindering their willingness to meaningfully participate in democratic processes. The UN Special Rapporteur on the freedom of peaceful assembly and association has raised concerns about the increased use of digital surveillance tools in the context of peaceful assembly.

6.3 Scottish Ministers, Police Scotland, and other relevant decision makers must adopt and implement an approach that embeds and mainstreams equality and human rights into the use of new technology in policing. This includes incorporating equality and human rights legal frameworks and principles into new legislation, codes of practice and guidance.

6.4 These governance issues have been raised by previous reports and groups in Scotland, including the Fraser Report, HMICS and the Biometrics IAG. The lengthy Justice Committee scrutiny of Biometrics raised these issues as well. Notwithstanding the current work of the IAG, the Cabinet Secretary's position that this issue of the legal basis for cyber kiosks should ultimately be settled by litigation is not consistent with a best practice philosophy, transparency or accountability.

6.5 The three milestones on Police Scotland's recent engagement with biometrics and emerging technology echo this. While the appointment of the Biometrics Commissioner for Scotland is further movement towards fulfilment of these ideals, the effectiveness of the role remains to be seen. In the meantime Police Scotland as the bearers of specific equality and human rights duties, must ensure non-discrimination, advances equality and fosters good relations.

6.6 The Scottish Police Authority established a working group to consider options for the future delivery, accreditation, oversight and governance of digital forensics in Scotland. This working group focused on operational structures and human rights within frameworks external to Police Scotland. However notable absences were recommendations that Police Scotland take operational steps to incorporate human rights within its internal ethical and operational frameworks, for example by adopting a human rights based approach.

6.7 As set out in Section 3 of this report, Police Scotland have been establishing ethics panels at local, national and overarching levels. However, this process has been delayed by the COVID pandemic.

6.8 The Biometrics IAG provided both a human rights analysis and a draft Code of Practice arising out of this. Their analysis incorporated the Scottish Human Rights Commission PANEL principles, and the Code therefore functionally reflects these. As the group set out, their consideration included technologies associated with biometrics which are many of the technologies that are emerging for policing purposes. The code therefore has use beyond DNA, fingerprints and photographs. Indeed, digital forensics such as facial recognition and cyber kiosks have been specifically identified as being within the remit of the report because of the extent to which they engage with identifiable personal data. The EHRC's submission to the consultation on the draft Code of Practice welcomed the references to the PSED and recommended that this should be strengthened by:

a) Making specific reference to the duty to assess and review the equality impact of proposed new or revised policies and practices when they are at their developmental stage;
b) Clearly setting out the different forms of prohibited conduct defined in EA 2010; and
c) Ensuring the associated complaints procedure is accessible and inclusive, with both on and offline means of engaging, and reasonable adjustments made where appropriate.

6.9 In ECtHR jurisprudence, in particular the *Weber* case from 2006, the Court has set out minimum standards for use in legislation governing the interception of communications on the basis that Art 8 is engaged. This included detailing the procedure to be followed for examining, using and storing the data obtained and the legislation should also include the precautions to be taken when communicating the data to other parties (*Weber (2006) E.C.H.R. 1173* at [95].). Earlier decisions had been strikingly specific in setting out these standards for police including a rubric of 6 minimum criteria (*Valenzuela Contreras (1999) 28 E.H.R.R. 483* at [46].).

6.10 Drawing on the jurisprudence across common law jurisdictions it appears that there would be an advantage to Police Scotland in considering that Article 8 is engaged wherever their technology is used to collect data that could on its own, or in conjunction with other data, identify people or personal characteristics. This includes any type of surveillance whether general or targeted. The engagement of Article 8 introduces a body of jurisprudence that has a strong basis in international law and parallels with common law jurisdictions such as Canada. ECHR makes it of fundamental importance to the legality of any action taken by Police Scotland.

6.11 An additional potentially useful endeavour would be for Police Scotland to formally commit to taking, and further embedding and enhancing, a human rights-based approach, particularly in evaluating any use of emerging technology or change of use of existing technology. PANEL is not a new approach for Police Scotland. They have had this tool recommended to them numerous times by the Scottish Human Rights Commission and others. Through collaboration and capacity

building, senior officers in Police Scotland and the SPA have been introduced to PANEL in contexts specific to Policing. In 2014 Police Scotland was heavily involved in compiling Scotland's National Action Plan for Human Rights and in that context, committed to identify[ing] opportunities to further embed human rights within the structures and culture of policing, including strengthening accountability for the respect of human rights as well as training on human rights for the police. It would, for example, help ensure legality and proportionality in the use of force and stop and search by Police Scotland through adequate training and monitoring, including the collection of disaggregated statistics.

6.12 Police Scotland practices already embody elements of a human rights based approach, such as public consultation, accountability to SPA and HMICS. However this could be further embedded and enhanced. Knowledge and understanding have been disparate and unsystematic. Much of the critique of the handling of Cyber kiosks was about the lack of a systemic approach to an area that clearly engaged equality and human rights. While individual officers were accounting for Police Scotland's performance, it became clear that there was no central understanding of the equality and human rights issues involved, nor did Police Scotland retain the resource to build human rights capacity. As noted above, there is no evidence that the SPA did either. What the PSED and PANEL offers are two authoritative frameworks for decision-making in relation to operations and behaviours. SHRC recommends that Policing should further embed human rights standards within five broad areas:

- Policy and strategic decision making;
- Operational planning and deployment;
- Training and guidance;
- Use and control; and
- Investigation, monitoring and scrutiny.

6.13 As part of meeting the requirements of the PSED equality should also be embedded in these areas.

6.14 This includes, by implication procurement of technology and the resourcing of its continuous use by Police Scotland. There is no aspect of these five areas that does not incorporate emerging technologies. Rather than consider them a niche or bespoke area, Police Scotland has an opportunity to centralise the issue while demonstrating its commitment to human rights. Police Scotland have been responsive to human rights concerns over issues such as the creation of a single police force, Stop and Search practices, Taser use, Scottish Biometrics Commissioners Bill, Facial Recognition and Cyber kiosks. The common thread here is a lack of human rights-based decision-making which has necessitated corrective action in response to external pressure. This fails to embody best practices in policing and is contrary to the wider duty to respect protect and fulfil human rights.

6.15 A formal commitment to adopting, implementing and enhancing an equality and human rights based approach in this area would ideally be accomplished through internalising human rights knowledge and capacity. For example Police Scotland could employ equality and human rights experts in order to assist in policy

design, analysis and assessment. By delivering equality and human rights knowledge, training and support to senior officers these experts would be embedding and mainstreaming such knowledge at every rank and in every aspect of policing. An organisation that places equality and human rights as a fundamental element of its function ought to be considerably well versed in equality and human rights based practices, to the extent that a complete equality and human rights impact assessment including a legal basis should be immediately available in a way that has been lacking.

6.16 Police Scotland, the Scottish Police Authority and the Police Investigations and Review Commissioner must comply with the SBC's code of practice when exercising functions related to biometrics. A court or tribunal in civil or criminal proceedings must take the code of practice into account when determining any question to which the code is relevant. That a clear set of principles for the management of biometric data is required is unanimously agreed. The Draft code meets the approval of a broad spectrum of experts including some within Police Scotland and the Scottish Police Authority and is therefore authoritative and of a high standard. The code was included in the public consultation on the Scottish Biometrics Commissioner Bill and the evaluation of the consultation reported good engagement with the code

.

6.17 It has been pointed out that public trust and confidence would be damaged without considered consultation and debate where there were complex legal, ethical and societal challenges to be resolved. It must be acknowledged that policing through intrusive technologies is a departure from the core democratic value of policing by consent. What Cyber kiosks, facial recognition, algorithmic policing all have in common is that these are privacy intrusive technologies that require careful use. Deployment is only lawful where the processing is fair, necessary and proportionate response to a pressing social need and where a robust risk assessment with sufficient mitigations have been completed. These assessments should be completed prior to any decisions about whether to deploy or not for any given purpose. Police Scotland must seek ever stronger safeguards to preserve the public trust that they rely upon in all of their functions when considering the use of emerging technologies such as these.

Recommendations

7.1 At a discursive level, observing the above examples of technologies and the subsequent lessons learned, there is a clear notion which challenges the rhetoric of techno-optimism which is found around the world in numerous sectors. Police Scotland have shown in their own 'lessons learned' that examples of emerging technology in itself do not offer a solution to social problems such as crime prevention, and public and officer safety – rather there is the mature and more energising comprehension drawn out from past implementations that technology should be thought of as 'an enabler' and a system of tools to assist in police work to gain new insights or overcome ineffective shortcomings inherited by analogue technologies. Drawing on the previous sections, we present our recommendations here:

1. **The continued implementation and reinforcement of a human rights-based approach to policing in Scotland**

Police Scotland should continue to embrace and implement a human-rights based, ethical and proportionate model for police use of technologies, in accordance with international best practices and with community input and engagement.

These international best practices include European Convention on Human Rights and their interpretation by the European Court of Human Rights and should be adhered to by Police Scotland regardless of whether the UK decides to repeal the Human Rights Act and/or leave the European Convention on Human Rights. In such a case, action by the Scottish Government may be required e.g. to incorporate these provisions into Scots law if possible.

This approach should include Police Scotland providing more analysis and engagement of human rights and equalities with technology use; specific references to Police Scotland's duty to assess and review relevant equality impacts of policies on technologies when at a developmental stage. The enhanced human rights-based and ethical approach should take place across the following domains: Policy and strategic decision making; Operational planning and deployment; Training and guidance; Use and control; and Investigation, monitoring and scrutiny. We recommend Police Scotland formally commit to adopting this approach which would ideally be accomplished through further internalising human rights knowledge and capacity. For example Police Scotland could employ equality and human rights experts in order to assist in policy design, analysis and assessment.

2. **Further consideration of impacts on new technologies on human rights and equalities needed**

The impacts of new technologies specifically on human rights and equalities need to be further considered. A multi-level analysis of rights and equalities impacts should be taken into account to embed and enhance Police Scotland practice, I.e. looking at

the impact at the individual, community and societal levels. There are existing requirements under data protection law (Data Protection by Design and Default, Data Protection Impact Assessment) that place an obligation on controllers to ensure that the data protection principles are adhered to and that any impact on individual rights and freedoms are identified, assessed and mitigated. There are also existing relevant obligations under equalities law and human rights legislation. In this recommendation we seek to aid compliance and raise the bar. In terms of raising the bar from a data protection point of view, specific actions could ensure that: Data Protection Impact Assessments (DPIAs) are developed alongside Equality and Human Rights Impact Assessments (EqHRIAs) and Children's Rights and Wellbeing Impact Assessments (CRWIAs), that Police Scotland refer to the ICO's Overview of Data Protection Harms when considering risks associated with processing and ensure that risks to individual's rights and freedoms are fully considered, assessed and mitigated in DPIAs. Further that these risks should continue to be identified, assessed and mitigated throughout the lifecycle of a new technology (i.e. not only at the 'developmental stage'). From an equalities and human rights perspective, Police Scotland need to assure themselves when undertaking Equality and Human Rights Impact Assessments (EqHRIAs) that any proposals are compliant with the Human Rights Act 1998 and the Equality Act 2010, and also satisfy the requirements of the Equality Act 2010 (Specific Duties) (Scotland) Regulations 2012, including the duty to assess the impact of applying new or revised policy or practice and publishing the results of these assessments in a manner that is accessible.

3. **Strong democratic engagement and consultation processes should be used to gain insights from the communities that a police service works for.**

These communities should include engagement with the protected groups defined in Equality Act 2010. In Scotland, if policing is to be done with public acceptance and agreement, then the public should be involved in changes to the policing system which could change the fabric of society, effect social relations, or impact democratic values. Complaints processes involving police use of technology must be accessible to all members of the public including those with disabilities.

4. **Legal basis for using policing powers vis-a-vis technologies must be clearly specified and shared with key stakeholders**

Police Scotland need to be able to demonstrate that the application of the policing power as set out in law must be clear and foreseeable and refer to and use proportionality and necessity testing; accurate and reliable/scientific standards, EqHRIA and community impact assessments. Although Police Scotland do specify the legal basis in DPIAs, given the potential for differing interpretations, legal basis (and opinions being drawn on) should be shared with key stakeholders as a matter of course in order that they may be questioned and tested and this must be reviewed in light of further developments (such as change in use case or additional information coming to light). Police Scotland need to be able to understand and articulate to diverse stakeholders the power which comes from the specific law which sanctions the use of a technology and refer to and use proportionality and necessity testing; accurate and reliable/scientific standards, EqHRIA and community impact

assessments. There should be more transparency with regards to the legal basis of police use of technologies and awareness raising with the public.

5. Further clarifications of legal basis via legislation or code of practice may be desirable

Further clarifications of legal basis for police use of technologies may be desirable, such as through legislation or a code of practice as we see for biometrics. Government should consider whether additional statutory codes of practice may be required to provide greater clarity and safeguards on the application of new technologies. Such new technologies might include AI for which a binding code for policing use may be desirable.

6. Special regard for the interests of children and vulnerable persons

When using new technologies in this context, law enforcement actors must have special regard to the interests of children and vulnerable persons and how the technologies may impact upon them. We recommend that Police Scotland conduct, embed and enhance Children's Rights and Wellbeing Impact Assessments (CRWIAs) alongside DPIAs and EqHIAs

7. More communication with the public and other stakeholders about police technology

Communication with the public and other stakeholders is needed about police technology capabilities and substantial changes to the dynamic of police work mediated by technology. This communication must be clear, publicly facing and speak equitably to a broad range of publics. Doing this is important both in terms of understanding and mitigating potential risks and harms but also ensuring fairness. The use of new technologies should not unjustly adversely impact an individual or group of individuals (which may potentially be discriminatory under the Equality Act 2010) and the processing should be within the reasonable expectations of the public.

8. Unacceptably risky technologies

Police Scotland should consider that in some cases a technology may be too controversial and pose unacceptably high risks to use even if there may be a legal basis for using it. A current example may be live facial recognition. Not using certain technologies and applications must be an option. Police and other actors in government should seek to understand why such technologies are considered controversial and risky and draw on lessons learned. Further work needs to be done on how unacceptability of risk may be assessed. Regard could be paid to the EU's proposed AI Act framework for risk in doing this. A category of 'unacceptable risk' could be added to Police Scotland's data ethics process to add to the current low, medium and high risk categories. In addition or as an alternative, the Scottish Government and Parliament could enact legislation defining what unacceptable risk means and designating technologies or application which pose such risks, e.g. those

systems whose use is intrinsically incompatible with human dignity (similar to the categorical prohibition of torture).

9. Ongoing evaluations and reflections on police use of technology

Police Scotland should continue to evaluate and reflect on its uses of technologies, recognising lessons learnt and the implementation of measures such as ethics panels, improved internal processes, engagement, transparency and external evaluations.

10. Drone awareness and impact

Police Scotland should raise awareness of its use of drones among the general public, clearly communicate to the general public how and when drones are deployed and how personal data is processed and should publish its draft Code of Practice on the use of drones and impact assessments, including the technical capacity of drone platforms to ensure privacy and data protection by design. Future Scottish Government Crime and Justice Surveys could include questions to benchmark awareness and attitudes of drones. The necessity of drone deployment rather than other means of investigation must be explained and justified by Police Scotland given the likelihood drones will capture sensitive personal data and have a high risk of collateral intrusion. Police Scotland should ensure that drone footage secured in criminal investigations from other parties, whether other public bodies, commercial organisations or others complies with the relevant legal and ethical safeguards.

11. Cross-border dialogues

Police Scotland should look across borders to access and share learning about best practice and acceptable use of new technologies. Evidence collected in trials, risk assessment and ethical studies elsewhere in the UK and further afield may be particularly helpful.

12. Lessons learned forum for police within the UK

A ‘lessons learned’ forum/knowledge exchange event could be established for police in Scotland, along with police in other parts of the UK, to share, showcase and discuss organisational knowledge from previous endeavours. This would mitigate continual institutional failures or mistakes relating to ethical and legal concerns, and allow best practice to be communicated in a transparent and open manner.

13. Continued enhanced risk management

Police Scotland should continue to enhance its approach to ensure effective and mature risk management processes (note link to workstream 4) to scope, map, identify and address any risk, opportunity or issue which may become associated with the adoption of a new technology, and continue to reassess and evaluate risks throughout the lifecycle of any new technology. With this risk-based approach to

understanding contexts and stakeholders, there should be greater emphasis placed on considering future impacts of technology and ways to understand how communities will respond to proposals. Evaluating risks throughout the lifecycle of the technology will also allow Police Scotland to act on risks which only become evident after the technology is deployed.

14. Technology procurement and provenance

More attention should be paid to the procurement and provenance of the technologies used by Police Scotland. In order to ensure enhanced cyber- and data security, the police and public sector more widely may need to consider developing technology solutions in-house rather than outsourcing them to private companies. Police Scotland should ensure that there are robust procurement processes in place to ensure that procured technologies are compliant with existing data protection, human rights and equalities obligations. National standards or a national Code of Conduct setting out these standards may be helpful here. Any proposed technology procurement project should follow the HM Treasury Green Book's business case framework, and make public an abridged version which includes an account of ethical issues. Where the police and public sector are developing technology solutions in-house rather than outsourcing to private companies robust design guidance that facilitates a data protection by design and default approach should be in place. A system of independent quality checking of such technologies may be desirable.

15. Police data sharing

More attention should be paid to the sharing of personal data generated by technologies used by police. Further safeguards may be needed for data sharing with other agencies and retention periods. There should be a review of the rules on retention considering questions of utility, lawfulness, proportionality and necessity. Rules around data sharing for the police should be legislated. A separate regime for children's data compared to that of adults may be advisable too. More research and discussion is needed on this topic, with the possible outcomes of further guidance, legislation and/or policy from relevant bodies such as the Scottish Government, Scottish Biometrics Commissioner and the ICO.

16. Biometrics transparency

More information could be published by Police Scotland publicly about biometrics they hold, for instance how many images they hold. The minutes of the Biometrics Oversight Board should also be published.

17. Evaluation of new Biometrics Commissioner

The establishment and effectiveness of the new Biometrics Commissioner in safeguarding human rights and upholding high ethical standards should be evaluated. There is already a reporting mechanism in the Scottish Biometrics Commissioner Act (SBCA) 20202 (section 6). We reiterate the need for this reporting

to be done in a way which involves wide consultation with relevant stakeholder groups and the public. We also consider that there should be a review of areas of police technology usage not currently covered by the SBCA, for the consideration of further policy, legislative and guidance reform.

Membership

- Professor Angela Daly, University of Dundee – Work Stream 1 Lead
- Tatora Mukushi, Academic
- Diego Quiroz, Scottish Biometrics Commissioner's Office
- Professor Burkhard Schafer, University of Edinburgh
- Denis Hamill, Police Scotland
- Andrew Alexander, Law Society of Scotland
- Professor Liz Aston, Edinburgh Napier University
- Jenny Brotchie, Information Commissioner's Office
- Bill Stevenson, Equality and Human Rights Commission
- Dr Marion Oswald, Northumbria University
- Stephen Ferguson, Crown Office and Procurator Fiscal Service

This report was written by workstream 1 members with administrative and organisational support provided by the Scottish Government Secretariat.

This publication is available at **www.gov.scot**

Any enquiries regarding this publication should be sent to us at

The Scottish Government
St Andrew's House
Edinburgh
EH1 3DG

ISBN: 978-1-80525-347-1 (web only)

Published by The Scottish Government, February 2023

Produced for The Scottish Government by APS Group Scotland, 21 Tennant Street, Edinburgh EH6 5NA
PPDAS1206882 (02/23)

w w w . g o v . s c o t