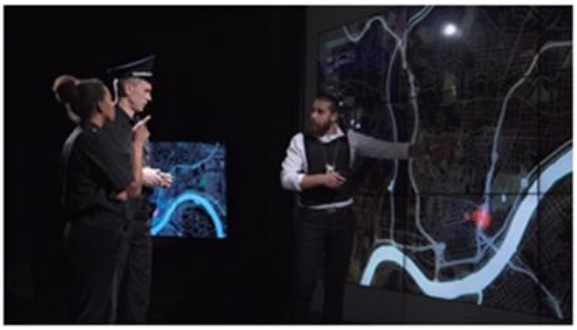

Independent review –
Independent advisory group on new and emerging technologies in policing

---

Final report

February 2023

Scottish Government
Riaghaltas na h-Alba

Contents

Foreword

This report explores a rights based, transparent, evidence-based, legal, ethical and socially responsible approach to adopting emerging technologies in policing, in a manner that upholds public confidence and safety. Alongside the importance of legal frameworks centred on human rights, equalities and data protection, it highlights the consideration of ethical and social implications, the key role of research evidence, consultation and public engagement and scientific standards in technological innovation and the centrality of robust mechanisms to ensure oversight and scrutiny.

The report draws together the work the Independent Advisory Group on Emerging Technologies in Policing (ETIAG) undertaken collectively over the past two years. I am extremely grateful to the core ETIAG members for their invaluable expertise and input, and to the workstream members and leads who contributed to key focus area discussions and wrote workstream reports. Many thanks also to the academics at Stirling who undertook the research commission and prepared their report. I would particularly like to thank Ryan Paterson, Graham Thomson and all members of the Scottish Government who provided secretariat support to the ETIAG during its lifetime.

It was a pleasure to serve as Chair of this group and I hope that as well as providing useful recommendations that will bring improvements in Scotland to legislation, policy and practice in the area of emerging technologies in policing, the report will also be of interest internationally.

Professor Elizabeth Aston
Director, Scottish Institute for Policing Research
Professor of Criminology, Edinburgh Napier University

1. Executive summary

Background

Policing in Scotland is operating in a complex context where the methods used to commit crimes are rapidly changing, cybercrime is more prevalent and the expectations on policing to keep people safe continue to increase, whilst resourcing pressures also grow. Technology is embedded in our everyday lives and policing must embrace new technology in order to fulfil its statutory duties and improve the safety and wellbeing of individuals and communities. There is a need for evidence-based innovation and facilitation of technological adoption in policing, but ensuring this is legal, ethical and subject to effective oversight is central to public confidence and upholding people's rights.

Emerging technologies as a term may be used to describe a new technology, the evolution of an existing technology, technologies being combined into a new application, a new service area or facilitating emerging new informational relationships and ways of working (Connon et al., 2023: 10). They may have been recently introduced into a specific setting, be at point of implementation, trial, in development or envisioned but not yet in existence. Emerging technologies often have digital components, but are usually an assemblage combining a range of components or developments integrated into a new 'technology' or application.

Established in late 2020, the Independent Advisory Group on Emerging Technologies in Policing has brought together members from across academia, civil society, regulators and policing to explore, discuss and make recommendations which will further support the enhancement of policy and practice in this space. The remit of the IAG was to report on whether legal or ethical frameworks need to be updated, to explore best practice around adoption of emerging technologies and provide recommendations to address any identified issues. The IAG met ten times over the course of two years.

Four separate workstreams were established to progress the work of the IAG, drawing in additional members (see Appendix B) and we launched a 'Call for Evidence'. The workstreams each produced reports covering: Legal Framework and Ethical Standards (Daly et al., 2023); Evidence and Scientific Standards (Buchanan et al., 2023); Consultation and Public Engagement (Campbell et al., 2023); Oversight Scrutiny and Review (Ross et al., 2023). In addition, we commissioned independent research from a team at the University of Stirling who reviewed legal frameworks, impacts on rights and good practice (Connon et al., 2023). All five reports will be published on the Scottish Government ETIAG website along with this report.

The substantive chapters in this final report cover: research evidence; legal frameworks; social and ethical implications and good practices; consultation and public engagement; technological innovation and scientific standards; and oversight scrutiny and review.

Summary

The importance of adopting an evidence-based approach at various stages of the process, i.e. from public engagement and consultation, to business cases and decision making, right though to implementation and evaluation of intended and unintended outcomes of the use of new technologies in policing is clear. The research community can play an important role in facilitating research, assisting with reviewing the evidence base, supporting evidence-based decision making, evaluation, translating research into practice and supporting innovation.

With regulation and governance of design and development, emerging technologies such as Artificial Intelligence (AI) may be used to advance, rather than put at risk, equality and human rights. However, specific legal concerns currently exist in relation to automated decision making and the use of AI in predictive policing, surrounding transparency and potential to exacerbate bias and discrimination. Live facial recognition raises human rights (proportionality) concerns as well as being potentially discriminatory. An ethical and legal assessment framework should embrace an equality and human rights-based approach and would likely mitigate various legal and operational challenges and reduce risks to public trust and discrimination.

Various social and ethical issues are associated with emerging technologies in policing and a number of best practices highlighted involve ethical principles and guidelines, transparency and codes of practice. Ethical considerations can be difficult to operationalise in the domain of policing but Police Scotland has various processes in place and enhancements planned to address ethical issues, including Ethics Advisory Panels and the introduction of a new Data Ethics Framework.

Enabling informed and genuine public dialogue is important in to order to support trust and confidence in policing. Consideration must be given to clarity of purpose, inclusion and accessibility and a variety of engagement approaches. Consultation and engagement should occur early, be evidence-based, promote ongoing dialogue and be transparent.

Technology innovation requires sociotechnical change and organisational support and should be seen as a long-term process. As new technologies are developed it is important to put the needs of members of the public, particularly those who come in contact with the police at the centre of an innovation. Police should integrate with developing standards, including from outside policing.

Since 2019 there has been a great deal of progress to establish robust decision making and oversight processes, and in 2021 Police Scotland and the Scottish Police Authority (SPA) published a Memorandum of Understanding which takes steps to enhance transparent discussion, engagement and communication and informed decision making. Police Scotland's proposed new Data Ethics Framework also enhances governance arrangements before investment (including external challenge and advice) and introduces a sixth ethics and human rights case.

In conclusion, the IAG believes that Scotland is in a strong position to seize the opportunity to become world leading in adopting a rights based, ethical, evidence-based, consultative approach to innovation and adoption of emerging technologies in policing, within a robust oversight framework. The following recommendations aim to facilitate this.

Summary of recommendations

Theme 1: Business case development, implementation and processes

1. Policing bodies (Police Scotland and SPA FS) should continue to adhere to HM Treasury Green book guidance for the Strategic Case, ensuring an **assessment of the available evidence base** (benefits and dis-benefits) across jurisdictions and published research is included in the Case for Change section in the Business Case.

2. The **assessment of the Ethical and Human Rights Impact** of emerging technologies should be evidenced and a proportionate judgement for the implementation of technology should be included in Business Cases. This could take the form of a 6th Ethical and Human Rights Case, which should make full use of EQHRIA, (incorporating the legal requirement to pay due regard to the three needs of the Public Sector Equality Duty), DPIA, CRWIA, Fairer Scotland Duty and other Impact Assessments, independent expert advice, Ethics Advisory Panels, and the results from the new Data Ethics Governance Framework.

3. Policing bodies introducing emerging technologies, applied in a context which impacts how the public are policed, should develop (with external input) a clear and **publicly accessible Operational Practice Code**, ensuring compliance with relevant statutes or codes of practice.

4. Police Scotland should seek to implement their **Data Ethics Governance Framework**. Key stakeholders should be involved in internal review prior to implementation and an effectiveness review should be undertaken 12 months after roll-out to ascertain the benefits realised and lessons learned.

5. Project implementation should ensure appropriate **training** for officers who will be utilising or monitoring emerging technology (particularly AI enabled technologies), with a particular focus on equality, human rights and data protection obligations.

6. When developing future proposals for technology use, policing bodies should consider, where appropriate, utilising small **tests of change/pilots** which could be externally evaluated to inform Business Cases and shape wider scale implementation.

7. When adopting emerging technology, policing bodies should ensure **standards** are designed to meet the needs of users and enable interoperability, compliance with data protection, equalities and human rights law, adherence to ISO, scientific and other relevant standards and codes. They could consider establishing a national technology clearing house to ensure robust scientific standards for AI technologies and an Algorithmic Impact Assessment policy.

8. Police Scotland should continue to enhance its approach to ensuring effective and mature **risk management** processes by scoping, mapping, identifying and addressing any risk (particularly risks to rights and freedoms of individuals), opportunity or issue which may become associated with the adoption of an emerging technology and continuing to re-assess and evaluate risks throughout the lifecycle.

Theme 2: Transparency, engagement and evaluation

9. Police Scotland should continue to develop and implement the **Consultation and Engagement Framework** described in this report when considering the adoption of emerging technology.

10. Police Scotland should clearly specify the **legal basis** for using emerging technology, share it with key stakeholders for input and publicly share it.

11. As part of the lifetime management of a new technology/project, policing bodies should have a clear **evaluation plan** which seeks to gather data (including baseline measurements) so that the emerging risks and efficacy can be assessed.

Theme 3: Legislation and policy

12. Whilst significant legislative gaps were not found, Scottish Government (and where appropriate the Scottish Biometrics Commissioner) should keep the legislative landscape under review and consider whether future technological deployments (such as Live Facial Recognition and certain applications of AI, e.g. in predictive policing) would benefit from the introduction of **statutory codes of practice** to provide greater clarity and safeguards. The possibility that certain applications of some technologies in policing should be categorically prohibited should be considered by Government.

13. The Scottish Government should take the learning from the *'Draft Proposals for Oversight of Ethical Considerations in Policing'* and consider endorsing a similar approach to enhancement of the Scottish Public Finance Manual as good practice across all public bodies in Scotland.

14. Policing bodies' (Police Scotland, SPA and PIRC) **complaints processes** must be clearly communicated prior to the start of new technology initiatives in policing and be accessible to all members of the public including those with disabilities. Where an adverse human rights impact to a person is the direct result of implementation of a new technology, those responsible for its implementation should provide an **effective remedy**.

15. Policing bodies should, at an early stage of the introduction of technology, ensure that **data flows** and the roles and responsibilities of all relevant parties under data protection law are mapped and understood.

Theme 4: Oversight

16. The SPA (and other oversight bodies) should continue to require assurance that **external evidence, research and advice** has been sought and considered in the development of cases and that engagement with partners and the public has been undertaken to inform the approach to embedding specific technologies in policing.

17. The SPA (and other oversight bodies) should continue to implement a system to **regularly review** the assessment of the public benefit, any risks, harms, positive or negative impacts of the introduction and use of emerging technology projects.

18. Policing and oversight bodies should consider the routine **collection, publication and accessibility of data** on the equality and human rights impacts of police use of emerging technologies in order to facilitate ongoing scrutiny and review.

2. Background

Introduction

Policing in Scotland is operating in a complex context where the methods used to commit crimes are changing rapidly, cybercrime is more prevalent and the expectations on policing to keep people safe continue to increase, whilst resourcing pressures also grow. Technology is embedded in our everyday lives and policing must embrace new technology in order to fulfil its statutory duties and improve the safety and wellbeing of individuals and communities. There is a need for evidence-based innovation and technological adoption in policing, but ensuring this is legal, ethical and subject to effective oversight is central to public confidence and upholding people's rights.

When it comes to the adoption of new technologies in policing various challenges have been evident in the Scottish context, although some important steps have been taken recently to learn from this and bring improvements. Policing in Scotland is, by its own admission, behind the curve when it comes to technological adoption but this presents an opportunity to learn from elsewhere, take stock and map out an improved framework.

As Bowling and Iyer argued, in relation to body worn video:

> 'the introduction of technology is happening before legislators and society at large have had the chance to reflect on the consequences; the mechanisms required to ensure technology is used with appropriate transparency, fairness and accountability are not yet in place' (Bowling and Iyer, 2019: 156).

On 13 June 2019, the then Cabinet Secretary for Justice, Humza Yousaf MSP, appeared before the Scottish Parliament's Justice Sub-Committee on Policing in relation to their report on Police Scotland's use of digital triage devices (also known as 'Cyber Kiosks'). Mr Yousaf indicated that he intended to form an independent advisory group on emerging technologies in policing, stating:

> *"Because of my commitment to the legal, ethical and proportionate use of new technologies…I plan to form an independently chaired reference group to scope the possible legal and ethical issues arising from emerging technological developments. The overall aim is to ensure that Police Scotland can continue to have not only the power to keep our communities safe but, crucially, the right safeguards to protect the rights of the individual."*

This announcement was made in the context of extensive parliamentary scrutiny of police use of technology in Scotland (e.g. JSCoP, 2019). In relation to digital triage devices, for example, the police had not conducted human rights and data protection impact assessments in advance. The extensive scrutiny by parliament in this space at the time was arguably symptomatic of weak oversight from the Scottish Police Authority (SPA) in 2018. However, there was then a significant delay in establishing the Independent Advisory Group

(due to a number of factors including the COVID-19 pandemic) and since 2019 significant improvements have been made to both policing processes and oversight by the SPA.

Established in late 2020, ETIAG (henceforth referred to as the IAG) has brought together members from across academia, civil society, regulators and policing to explore, discuss and make recommendations which will further support the enhancement of policy and practice in this space. The IAG believes that Scotland is in a strong position to seize the opportunity to become world leading in adopting a rights based, ethical, evidence-based, consultative approach with a robust oversight framework in relation to the adoption of emerging technologies in policing.

The final report of the IAG is structured as follows. This background section maps out the terms of reference, membership and activity (including evidence gathering) and provides a definition of emerging technologies.

The first substantive chapter focuses on the role of **research evidence** in decision making and evaluation relating to the adoption and implementation of emerging technologies in policing.

The next chapter covers **legal frameworks** (human rights, equalities, data protection and law of evidence), impacts on individuals' rights, processes (including impact assessments) and procedures; lessons learned, good practices and legislative gaps.

Chapter five covers ethical considerations, including the use of ethics panels and lessons learned in Scotland, **social and ethical implications, and good practices** in ethical frameworks from other fields and jurisdictions.

The sixth chapter uses a range of literature, best practice and learning from experiences in Scottish policing and elsewhere to develop an evidence base and framework for **consultation and public engagement** that sets out proposed principles and practice for clear, meaningful, accessible and appropriate approaches to engage on emerging technologies in policing.

The next chapter on **technological innovation and scientific standards** looks at barriers and facilitators to adoption; viewpoints of technology providers on the future horizon for technological innovation and requirements in relation to scientific standards. This includes looking at data driven innovation; the place of the needs of victims and other members of the public in technology adoption; data interoperability and standards; and a consideration of what next generation standards for digital evidence management may look like.

Chapter eight on **oversight, scrutiny and review** provides an overview of existing decision making, oversight and scrutiny framework that is in place to support the assessment of the potential adoption of new technology across the policing system in Scotland, highlights recent steps to bring improvements and proposes further potential routes to enhancement. It follows the consideration and decision making pathway of technology adoption from initial concept assessment, case for change development, decision making, governance approvals, project delivery and into business as usual adoption.

The final chapter of the report draws some conclusions and outlines the final recommendations of the IAG.

2.1 Terms of reference

The remit of the Independent Advisory Group was to investigate and report to the Cabinet Secretary for Justice and Veterans on whether the current legal or ethical frameworks need to be updated in order to ensure Police Scotland's use of emerging technologies in relation to operational policing is compatible with equality and human rights and other applicable legislation. The IAG would also look at current best practice around new technology; and to provide specific recommendations or potential outputs to address any identified issues.

It was anticipated that the review would:

- Consider what potential impact emerging technologies or analytical techniques - either currently available or in development, but not presently deployed - could have on Police Scotland's detection and prevention of crime.
- Consider the extent to which the use of such emerging technologies or analytical techniques by Police Scotland is compliant both in application and in spirit with equality and human rights obligations, including those set out in the Human Rights Act 1988, the Scotland Act 1998 and the Equality Act 2010.
- Determine whether the current legislative framework used by Police Scotland to exercise their powers is sufficiently robust to allow for the proportionate and justifiable deployment of such technologies or techniques. This will be considered within the context of the Police and Fire Reform (Scotland) Act 2012 which focuses on public safety and wellbeing as well as the prevention of crime. Human rights, equality, data protection and other relevant legislation will be considered in this area.
- Draw on a wide range of evidence from Scotland and other jurisdictions in order to ensure that, as far as possible, any possible recommendations are forward and outward looking and future proofed.
- Determine whether the range of ethical frameworks used by Police Scotland and other policing and public sector bodies are sufficiently robust to allow for the proportionate and justifiable deployment of such technologies or techniques.
- Explore whether there are suitable institutional oversight functions to oversee the introduction of new technologies and consider in what circumstances policing bodies should seek to engage, consult and bring in independent bodies regarding the use of new technology.
- Ensure that the Group's focus, and any associated recommendations, take cognisance of the existing and planned landscape of advisory and regulatory bodies, including but not limited to the Investigatory Powers Commission and the Biometrics and Forensics Ethics Group.

2.2 The advisory group

The Independent Advisory Group consisted of the following members:

- Professor Elizabeth Aston, Edinburgh Napier University (Chair)
- Professor Angela Daly, University of Dundee
- Jenny Brotchie, Information Commissioner's Office (advisory role)
- Professor Bill Buchanan, Edinburgh Napier University
- Diego Quiroz, Scottish Biometrics Commissioner's Office
- Bill Stevenson, Equality and Human Rights Commission
- Barry Sillers, Scottish Police Authority

- Professor Burkhard Schafer, University of Edinburgh
- Georgie Henley, techUK
- Andrew Hendry, Chief Digital Information Officer for Police Scotland
- Elaine Galbraith/Craig Naylor, His Majesty's Inspectorate of Constabulary in Scotland
- Ken Dalling, Past President of the Law Society of Scotland
- Stephen Ferguson, The Crown Office and Procurator Fiscal Service

In addition, earlier on in the process we had other organisations who contributed to the work of the IAG e.g.: Scottish Human Rights Commission and Open Rights Group, Scotland. Other invited organisations (Convention of Scottish Local Authorities, Amnesty International, Empowering Scotland's Ethnic and Cultural Minorities etc.) were unfortunately unable to contribute to the work of the group for various reasons.

The secretariat consisted of officials from the Scottish Government.

Advisory group workstreams

Four separate workstreams were established to assist with the work of the Advisory Group. For a full list of workstream members please see Appendix B. Each workstream developed their own work programme and produced a report based on the following remits:

- **Legal framework & ethical standards -** to consider existing legal frameworks, ethical panels etc. and explore good practices and gaps in relation to both legal frameworks and ethical standards.

- **Evidence and scientific standards -** to consider the role of research evidence in the consideration, adoption and implementation of emerging technologies, to explore barriers and facilitators to research and innovation and consider best practice in scientific standards relating to adoption of technology in policing.

- **Consultation and public engagement -** to consider the role of consultation and public engagement in supporting police legitimacy, consent and public confidence as new and emerging technologies are considered which change operational policing in Scotland.

- **Oversight, scrutiny and review -** to identify and/or document existing oversight, scrutiny and review mechanism and map any gaps in this area.

2.3 Interim report

We produced an interim report which was submitted on 24th June 2022. In it, we explained the work undertaken to find evidence to assist us to produce our final report, with conclusions and recommendations based on this evidence.

In addition to providing an update on the progress of the workstreams and key emergent themes, we described the two key ways in which we gathered evidence –a formal Call for Evidence and Commissioned Research. The delay in securing appropriate research on this topic was, along with the pandemic, the main reason for seeking an extension of time from the current Cabinet Secretary for Justice and Veterans, Keith Brown MSP, to allow the research team to fully complete their work and for the group to make the most of the

important evidence which has been provided to help us to identify conclusions and recommendations. With that extension, the final report is being submitted to the Cabinet Secretary by the end of November 2022. Obviously, we appreciate that the Cabinet Secretary will require some time to consider our report and the underlying evidence before issuing a response on behalf of the Scottish Government.

2.4 Evidence

Call for evidence

A Call for Evidence was launched by the IAG and was open between 5th July and 4th October 2021, with 13 responses being submitted during this period. These responses included technology companies and academics who have extensive experience in this field. We are grateful to all of those who took the time to respond and these have been analysed and used to inform the work of the group.

Research

The Independent Advisory Group also supplemented their own investigatory work by commissioning independent research through the Scottish Institute for Policing Research (SIPR). The project was awarded to a research team based in the University of Stirling - Dr Niall Hamilton-Smith (lead), Prof William Webster, Dr Mo Egan, Dr Diana Miranda, Dr Irena Connon and Niamh MacKay.

The research planned to support the IAG by:

- Detailing the relevant legal frameworks, processes and practices in Scotland
- Looking outward and exploring good practice from other jurisdictions and other fields, including a comparative look at legal frameworks and ethical standards
- What impacts on rights do individuals (including witnesses, victims, suspects and members of the public) experience as a result of the use of new and emerging technologies. Also, whether any groups are particularly affected and if the existing legislation provides sufficient safeguards against risks.
- Ascertain whether there are there any legislative gaps which need to be filled.

2.5 Definition of emerging technologies

As outlined in the IAG commissioned research report (Connon et al., 2023: 9-12) emerging technologies as a term may be used to describe a new technology, the evolution of an existing technology, planned implementation of a recently developed technology or potential implementation of technologies that are currently developing or are expected to be introduced in the next five to ten years.

The adoption of emerging digital technologies by public services can present both opportunities and risks to rights and freedoms, including through their innovative use of personal data. For public services involved in policing, legal, ethical and social challenges posed by digital technologies have implications for relations between the public and the state.

Connon et al. (2023) suggest that four key features of emerging technologies should be considered: the nature of the technology, the technological components, applicational elements and the point of emergence. Firstly, although in theory any physical object could

be considered a technology, in the contemporary context emerging technologies are usually assumed to have digital components (but they do not have to be exclusively digital and are often comprised of other elements) that support information flows involving data (including personal data). Secondly, it is important to note that an emergent technology is not usually a single technology but rather an assemblage combining a range of technological components or developments integrated into a new 'technology' or application. Thirdly, technologies may be considered emergent if they are being combined into a new application, a new service area or are facilitating emerging new informational relationships and ways of working. Finally, emerging technologies may have been recently introduced into a specific setting, be at point of implementation, trial, in development or envisioned but not yet in existence.

We also acknowledge that in order to ensure proper use of technology is facilitated, rather than inadvertently prohibited, it is important to be as clear as possible on the intended specific use cases of various technologies in policing. For example, Artificial Intelligence could be used in number of different ways in various policing contexts. However, sometimes the literature is not specific, and it may not be possible to envisage and therefore consider all potential intended use cases in policing.

Finally, we would like to highlight that our focus was on the application of new technologies on areas of policing that are within devolved competence of the Scottish Parliament (i.e. not covert policing technologies, Counter Terrorism applications etc.), since such devices and technologies, and their authority for use, and independent oversight, stems from legislation reserved to Westminster. Furthermore, where our recommendations refer to policing bodies we are focused on the Scottish context, i.e. Police Scotland, SPA Forensic Services and on policing oversight bodies such as SPA, Police Investigations and Review Commissioner (PIRC), His Majesty's Inspectorate of Constabulary (HMICS) and the Scottish Biometrics Commissioner (SBC).

2.6 Limitations and disclaimer

This final report reflects the work of the Chair, IAG members, workstream members and research team who have done their best given the time and resources available to them. Clearly, emerging technologies in policing is a vast topic so there were limits to the amount that could be covered by the group and in this report. For example, it is noted that given the remit of the group much of the analysis focuses on identifying issues (legislative gaps, social and ethical implications) to drive improvement, rather than highlighting the benefits of technology. However, we acknowledge that there is a balance to be sought in ensuring appropriate safeguards are in place, whilst also enabling policing to embrace new technologies in order that it may fulfil its statutory duties. Also, in places some of our commentary is quite general in mentioning technologies instead of considering their various specific use cases in policing, which we acknowledge would have been preferable but was not always possible.

Furthermore, we have generally analysed and commented on current legislative frameworks in force at the time of writing. This has excluded consideration of UK Government proposals to reform data protection and human rights in the forms of the Data Protection and Digital Information Bill and the Bill of Rights Bill. For data protection matters, we consider standards under the European Union General Data Protection Regulation and

Law Enforcement Directive (which are currently implemented in UK law) to be best practice and should continue to be followed by authorities in Scotland even if the Data Protection Act 2018 is repealed or reformed.

It is worth noting that this group was established during the COVID-19 pandemic, which put additional work and personal pressures (illness, childcare etc.) on individual members and organisations and impacted the work of the group and its timescales. Furthermore, some members were not in a position to contribute as much as hoped, some organisations had to withdraw and others declined invitations to join the group due to resourcing constraints. For example, this meant that the input from third sector and civil society organisations was not as strong hoped.

As the Chair of the IAG I have endeavoured to facilitate critical and constructive dialogue between members on this topic and I am pleased that we have managed to work together in an open, honest and respectful manner. This report represents the final output of the IAG. The recommendations do not necessarily reflect the views of the individual members, or of the individual organisations represented on the IAG, which may vary on certain issues.

3. Research evidence and emerging technologies in policing

This chapter focuses on the role of research evidence in relation to the adoption and implementation of emerging technologies in policing. This chapter draws largely from chapters 2 (and 4) of the workstream 2 report (Buchanan et al., 2023), with some content derived from the Stirling Research Commission (Connon et al., 2023) and other workstream reports, e.g. Campbell et al. (2023). Whilst the opinions and experiences of the public and stakeholders may also be of interest these are considered elsewhere, e.g. Chapter 6, whereas this chapter focuses on research evidence. It covers the use of research evidence in supporting decision making and evaluation, innovation, consultation and engagement and provides suggestions for further research.

Existing approaches to use of research evidence:

It is crucial to understand the full impact of emerging technology to enable appropriate decisions to be made before its implementation in Scottish policing.
The first section of the report draws on chapter 2 of the workstream 2 report (Buchanan et al., 2023) and considers existing approaches taken by Police Scotland to the use of research evidence for the consideration, adoption and implementation of emerging technologies. It provides an overview of the governance that is followed during the consideration of new and emerging technology prior to any subsequent adoption, following the pathway of technology adoption from initial idea/concept to Business-as-usual adoption of the technology.

Governance for technology adoption pathways:

Police Scotland and the Scottish Police Authority (SPA) have a governance process in place which has been maturing to maximise appropriate governance, oversight and scrutiny (see Figure 2.1 Buchanan et al. 2023: 5). This includes the recent introduction of a joint Memorandum of Understanding (see Chapter 8 below) between the two organisations, which aims to ensure early visibility and oversight of any new strategy, policy or practice under consideration by Police Scotland. Neither organisation has a specific board for consideration of new and emerging technology or research evidence, but the most likely governance route for emerging technologies would be through Police Scotland's Change Board or Demand, Design and Resources Board, into the Strategic Leadership Board and then on to the SPA Resources Committee and SPA Board (see Figure 2.2, Buchanan et al., 2023: 7).

SPA's function in oversight of change enables questioning of new initiatives. It is vital to understand ethical aspects of technologies and their potential use in policing prior to adoption (i.e. at the stage of considering need for change). It is also essential to understand the societal and cultural aspects of the need for change, and of the technology and its deployment and to consider the required socio-technical innovation. It is acknowledged that all these aspects need to be analysed and evaluated together, particularly since the

operational technologies deployed e.g. with the aim of identifying a suspect population, can aggravate inequality and distrust by drawing from in-built bias in data, technologies, practices and institutions. Unintended bias or inequality would be one of the aspects examined through the proposed sixth ethics and human rights case process (see Chapter 8). Furthermore, it is important to note that where a proposal to process personal data presents a likely high risk to the rights and freedoms to individuals there is an existing legal obligation to assess the risks to the rights and freedoms of data subjects and the measures envisaged to address those risk in a Data Protection Impact Assessment (DPIA) under data protection law.

Stage 1 is when the need for change is identified and considered. As a project can be initiated from any business area (Operational or Corporate). If the latter it will be approved by a Director, but if Operational Stage 2 is likely to involve the preparation of a brief for one of the Local Management Boards (Local Policing, Crime and Operational Support or DCC Designate). If a change is approved in principle by one of the boards, the lead will be asked to prepare a Potential Project Assessment (PPA) to present to the Demand Management Board where it may be deemed Business as Usual (BAU) or Project. If the latter an Initial Business Case (IBC) will be completed to bring together all of the key information needed to initiate the project. If it is of substantial size and scale a Programme Brief will also be required.

The IBC includes aspects such as the case for change, project plan, controls and communication plan and should include the benefits and dis-benefits of the proposed change. Crucially, 'benefits should be quantifiable wherever possible and be based on robust research and evidence' (Buchanan et al., 2023: 8). However, as it stands there is no mandated requirement for scientific research to be included as part of the IBC. Nonetheless, this seems to be changing as the SPA have stated that having dip sampled recent IBCs in 2022 it was 'common for there to be a strong reference made to existing scientific literature or evidence (with a particular focus on evidencing the benefits of proposed technology)'. In my view as Chair, some basic level of information about the research evidence base should be required for all business cases and it is important to ensure that the assessment be balanced and include evidence about 'dis-benefits' as well. This is not to say that new empirical research needs to be conducted (which can take significant time), but that the existing evidence base should be taken into account (see key consideration 3.1 below).

Stage 3 involves consideration of the IBC by Change Board of the benefits, impact, timescales, cost or resource implications etc. If approved a Full Business Case (FBC) will be prepared and considered by the relevant Programme Board and Change Board using the Investment Governance Framework (see Buchanan et al., 2023 Appendix A).

Whilst the business case template used by Police Scotland lends itself to the inclusion of research and evidence, particularly in the 'case for change' section, as Chair I note that the business case template does not explicitly mention research and evidence. The description includes a 'qualitative assessment of the status quo and benefits the change/proposal will bring' and encourages the inclusion of 'quantitative data and scientific standards' (including for use as baseline in any potential future evaluation). Detail of the current business case structure may be found in Table 2.1 (Buchanan et al., 2023: 10). Indeed, the dip sampling of business cases found that although it was common for there to be reference made to

existing literature or evidence of benefits there was a lack of scientific evidence and research provided to support the case for change.

Therefore, an opportunity exists to strengthen the business case process by mandating for the inclusion of evidence to substantiate the case for change. In my view as Chair this should include a range of the highest quality available research evidence, using the most appropriate methods to answer the question at hand. Wherever possible this should include any available quantitative data, although it its acknowledged that qualitative data may be most appropriate in certain circumstances. Crucially, to ensure balance, evidence must also be provided on any identified drawbacks or pitfalls associated with the implementation of the change. The level of risk should determine the level of evidence gathering required. Furthermore, consideration should be given as to whether a pilot should be conducted prior to roll-out of certain technological deployments in policing.

If the business case is approved the project will progress straight to Stage 5 (implementation) if it does not impact people's working conditions, or to *Stage 4 (consultation)* if it does. All Organisational Change proposals are presented to the Joint National Consultative Committee (JNCC), which has representation from staff associations, prior to any consultation with staff. Technology projects will not routinely go through this step, but some major technology projects may have organisational implications and therefore go through Stage 4. Following JNCC, consultations may begin, often in groups (before individual meetings with who are impacted) and provide the opportunity for staff to make any redundancy mitigation counter proposals. Consideration should be given to the fact that diversity and representation in decision making structures may be particularly important in relation to technology in policing, given the impact on protected characteristics such as race.

Once a project moves to *implementation* phase (Stage 5) consideration should be given to introducing controlled pilots and an evaluation process for the impact of new technologies. A baseline measurement should be confirmed ahead of the introduction of technology and ultimately be used to assess the implementation and its impact. Evaluation is also particularly important given the requirement for ongoing review of DPIAs under data protection law, as the actual risks and harms that may arise as a result of the deployment of a new technology will only become evident after deployment.

Policing research partnerships:

Policing Research Partnerships can play an important role in facilitating research, dissemination, knowledge exchange and impact. This can assist with reviewing the existing evidence base, shaping decision making and supporting evidence-based policing. It can also help with embedding evaluation (process or outcome evaluation) of technological adoption, providing a reflection of lessons learned in implementation, and assessment of benefits realised and any unintended consequences or harms.

SIPR is one such Policing Research Partnership, along with many others in the UK including the N8 Policing Research Partnership and other police-academic collaborations (e.g. the Open University) and university centres (e.g. Northumbria, UCL). Established in 2007 and supported during its initial five year phase by investment from the Scottish Funding Council and the Association of Chief Police Officers in Scotland, the Scottish Institute for Policing Research is a collaboration between Police Scotland, the SPA, and 14

Scottish universities. SIPR's mission is to support independent, multi-disciplinary policing research to enable evidence informed policy and practice.

The work of SIPR is advisory in nature, not decision making, but the intelligence and evidence gathered and generated is in a strong position to support several aspects of decision making, for example for Change Board, Strategic Leadership Board, SPA Board. SIPR may also be asked by Police Scotland and the SPA to assist in commissioning academic researchers to assist with reviewing the evidence base or considering the implications of the adoption of new and emerging technologies before implementation (e.g. Body Worn Video, BWV) or to evaluate the implementation of various technologies or approaches (e.g. Benefits of implementation of mobile devices with frontline officers in Police Scotland 2019-2020). There is no one formal route for this work to be commissioned but research typically transpires from discussions at committees (e.g SIPR Executive Committee), boards or with senior leaders. Consideration should be given to determining when an evaluation is needed, how it can be implemented ahead of the change happening and seeking SIPR's support in commissioning the evaluation prior to the technology coming into effect.

Other insights:

Police Scotland use the Citizen Space website to host consultations and engagement in order to gain an understanding of public opinion on a variety of issues. For example, it was recently used to gain understanding of public opinion on the use of BWV. A variety of other engagement approaches e.g. focus groups are also used (see Chapter 6).

Comparison with other comparable police forces may also provide valuable insights and benchmarking for decision making and evaluation. However, dip sampled business cases showed little comparison to how comparable new and emerging technologies had been implemented in similar police forces. This could be valuable evidence to include as part of the proposal for change and may also provide insights of lessons learned to inform implementation.

In conclusion, at present, although Police Scotland and the SPA have a governance process which may be used to oversee the implementation of emerging technology, there is no formalised inclusion of an assessment of the research evidence base in this process. Whilst reviews of the research evidence base may be undertaken in certain cases to inform the decision making or implementation of new technology (for example, BWV), there is no agreed process or criteria in place to formally require an assessment of the evidence base in the business case. This should therefore be included as part of the change process to enable the appropriate governance mechanisms to make informed decisions. Furthermore, it is crucial to consider the implications of new technology on the communities it impacts and ensure evaluation is in place where necessary. Engaging with external organisations and individuals from an early stage provides an opportunity to mitigate barriers to successful implementation early in the process, e.g. ICO guidance is that the DPIA process should involve consultation. Furthermore, in my view as Chair the level of evidence gathering required to inform decision making and whether new research or evaluation is needed or not will vary depending on the extant knowledge base and level of benefit or potential risk posed by the proposed technological adoption in policing in Scotland.

Research evidence & innovation:

Other chapters of the workstream 2 report (Buchanan et al., 2023) on technological innovation also have some useful insights of relevance to research evidence. In chapter 3 for example there is an acknowledgement that forming lasting partnership entities assists with better translating research into practice and with research and development investment for technology innovation. In addition, there is an acknowledgement that short-termism and a stop-and-start approach necessitates extra effort and funding over time to continue research and development. TechUK's contribution states that organisations who adopt a collaborative, consortia-based model may achieve better results than traditional 'ecosystem' approaches which may stifle agility, innovation and genuine engagement from experts. Although there are benefits to a consortia-based model the IAG acknowledges that procurement implications and conflicts of interest would need to be considered and mitigations put in place.

In chapter 4 techUK asked their members about evidence-based decision making and how the tech industry can engage with academia when developing evidence-based pilots. Their contribution acknowledges that evidence-based decision making, and policing research partnerships can assist police forces with connections, with achieving their intended outcomes, and result in more well researched policies and practices. When making informed decisions about the adoption of emerging technology in police organisations this may be done using a combination of best practice research evidence, industry knowledge and experience (by both policing and technology partners) and the experiences of the victims of crime (and others impacted by the criminal justice system).

There are a number of areas where academia, and the research community as a whole, can bring fresh insight into the process:

- 'Police practices should be based on scientific evidence about what works best and hence it is important that for any evidence-based pilot developing, industry must engage academia. Academia are keen to support the development, testing and promotion of innovative practice to help build the evidence-based solution and understand what would work best.' (Buchanan et al., 2023: 30).
- Partnerships, mentoring schemes, apprenticeships and test panels/groups which can road test new technologies and share ideas/challenges to ensure that new technologies are approached from an outcomes perspective.
- Research and evaluation may be used to inform or assess the adoption of technologies. For example, in 2019 SIPR supported Police Scotland in the run up to their commissioning an evaluation of the Digitally Enabled Policing Programme (DEPP), the 'Police Scotland Mobile Working Project' (MWP), which reported in 2020. This project equipped operational officers with a digital mobile policing solution to replace the traditional paper notebook and to provide remote, live access to key policing information systems. This is cited as a good example of how academia can assist and support the review of policing projects, whilst remaining independent and transparent. However, as Chair I would note that in order to safeguard the quality and independence of evaluation research it is important to ensure that where feasible a Research Advisory Group is established and ideally publications are peer reviewed. There are benefits to commissioning evaluations through a third party like SIPR, rather than by Police Scotland directly.
- Another example provided involves the The Digital First and GDS Service standards which emphasise (1) using evidence to quickly demonstrate that there is a good

understanding of the problem to be solved before making substantial commitments (2) using research with real users and real data to quickly establish whether a worthwhile solution can be delivered before undertaking significant development and (3) focussing on rapid, iterative prototyping against agreed KPIs to drive effective design.

Evidence-based consultation & public engagement:

As outlined in the workstream 3 report (Campbell et al., 2023) research evidence also has an important role to play in informing public engagement and consultation. As Campbell et al. (2023) states, supporting evidence and materials was one of the areas identified for further consideration based on a review of the approach to public engagement on BWV, undertaken in order understand key lessons for future engagement.

In the initial engagement on BWV, Police Scotland shared an evidence base of reports. Concerns were raised that this was not fully representative of a wider range of literature and views on the use of BWV. Indeed, I would like to note as Chair that in my role as SIPR Director I raised concerns with Police Scotland that the *short summary leading into the engagement exercise* stated that evidence showed that BWV achieves certain outcomes. The wording was changed to remove the reference to evidence when I pointed out that the statements did not align with the findings of a systematic review of the highest quality research evidence (Lum et al. 2019).

Campbell et al. (2023: 21-22) state that *'the design phase of future engagement approaches will consider evidence with key stakeholders and seek an independent view of the robustness of the materials being provided to the public, guided by senior responsible officers and Police Scotland's in-house Academic Research team, whilst engaging with research partners. This will ensure, as far as possible, an appropriate range of information and views are shared and that Police Scotland has sought independent consideration of the materials being published and presented.'*

The workstream 3 report also concludes that consideration could be given to adding to the evidence base of materials as suggestions are received from the public and groups taking part in the engagement/consultation. It is important that the materials being shared as part of the evidence base are fully accessible for all. Also, a user-centred approach must be taken to consider how someone gets to the online survey or consultation page and through which 'journey' /starting point, in order to ensure that there are multiple opportunities to engage with the evidence available to inform their views in advance of taking part. Beyond online consultations, various other engagement approaches appropriate to meeting the diverse needs of communities are used to encourage meaningful participation, see Chapter 6.

Finally, evidence and materials that support the engagement should represent a range of views to enable an open and transparent dialogue. Evidence and materials must be accessible and inclusive for a range of needs; to ensure that everyone is able to meaningfully participate in understanding the evidence and materials. Good practice would suggest producing 'easy read' versions of materials, and working with key partners who are experts on the subject to understand any tensions with any evidence being provided to inform decision-making. It is worth noting that the evidence base should also be referred to in a DPIA and it is good practice to publish DPIAs. Furthermore, equality legislation is even more prescriptive – The Equality Act 2010 (Specific Duties) (Scotland) Regulations 2012

describe how relevant evidence relating to persons who share a relevant protected characteristic must be considered, and that results (of the impact assessment) must be published in a manner that is accessible.

Furthermore, in my view as Chair in addition to making a range of materials available it would be important to develop (with input from independent stakeholders) a clear and succinct public facing summary of the existing research evidence (acknowledging any limitations and gaps in knowledge) to be shared during public engagement and consultation exercises and in the summary of the ethics and human rights case. Note the Scottish Biometrics Commission's process for introducing a new biometric technology or a new application of an existing biometric technology for policing and criminal justice purposes in Scotland (SBC CoP Appendix D) will need to be complied with for biometrics.

Suggested areas for further research:

The commissioned research report (Connan et al. 2023) makes a number of suggestions of potential areas which may warrant further research. These are listed below verbatim as they are covered in the commissioned report, but the IAG notes that there is a need to assess the strategic importance, level of risk, and potential value of the research for each of the proposed areas for further research in order to guide decision making on which areas should be prioritised for funding by various partners (Scottish Government, Police Scotland, Scottish Police Authority, the Scottish Institute for Policing Research etc.). It is also noted that in addition to guiding which areas may warrant prioritisation for funding, these suggestions will be informative to SIPR and the academic community who are keen to leverage external funding e.g. from research councils.

1. Suggestions for research relating to Electronic Database Technologies (Electronic database technologies represent one form of continually evolving technology that are used in contemporary police practice. Electronic databases store, organise and process information in a way that makes it easy to perform searches and analyses.)

a. Further research should be undertaken concerning the use of national datasets to gain a better understanding of the risks involved in the use of such technologies.
b. There is a need for greater integration between academic researchers, police, the policy community and third parties to develop and implement specific solutions for the embedding of these forms of technology in policing practice that are sensitive to the needs of all parties.
c. For more trials and assessments to be undertaken to establish best practice and decision making within a range of policing contexts in Scotland and the UK.

2. Suggestions for research relating to Biometric Identification Systems and Artificial Intelligence Technologies

a. The need for further research to be conducted to explore the benefits and limitations of the use of facial recognition technologies (of various kinds e.g. live or not) in different policing activities (namely, public order policing, crowds, and public events).
b. Development of a set of shared concepts and terminology to develop an ethics of algorithms and the building of a more rigorous evidence base for the discussion of social and ethical issues surrounding the use of AI in policing.

c. Consideration to be given to the statistical and scientific validity of proposed AI technologies and for context-specific evaluation methodologies to be applied for statistical algorithms.
d. The need to interrogate biases and limitations as to the efficiency of AI systems prior to development and use.
e. For police professionals and third parties that they work closely with (i.e. local authorities) to be involved in the design and implementation of these technologies to help promote ethical awareness and practice.

3. Suggestions for research relating to Surveillance Systems and Tracking Devices
a. If technologies are being contemplated consideration should be given to conducting research e.g. trials to explore the benefits and limitations of the use of these different forms of technology in different policing activities and contexts, e.g., in Scottish rural vs.urban contexts.

4. Suggestions for research relating to data protection, the law of evidence, and equality and human rights: applicable to all forms of emerging technologies
a. At the outset of designing, adapting, or adopting an emerging technology, consideration should be given to how that technology is to be used to ensure compliance with the law of evidence.
b. The roles and relationships under data protection law and data flows between all controllers and processors should be mapped out and understood prior to processing.
c. Further research should be undertaken to consider the legal and ethical implications for the use of emerging technologies in policing activities involving children, with a view to ensuring compliance with the United Nations Convention on the Rights of the Child.

Chapter 3 summary and conclusion

Decision making: It is crucial to have an understanding of the existing evidence base regarding the impacts of emerging technologies in order to enable appropriate decisions to be made regarding their adoption in Scottish policing. The governance process has been maturing, including the introduction of a joint Memorandum of Understanding between Police Scotland and the SPA, which aims to ensure early visibility and oversight of any new strategy, police or practice under consideration. Business cases form a key part of decision making and are expected to include an assessment of benefits of the proposed change. At present the inclusion of an assessment of the research evidence base is not explicitly required.

The research community, including policing research partnerships (e.g. the Scottish Institute for Policing Research, SIPR) can play an important role in facilitating research, assisting with reviewing the evidence base, supporting evidence-based decision making, evaluation, translating research into practice and supporting innovation. Other insights are also provided by Police Scotland, including for example the use of Citizen Space to gain an understanding of public opinion. Research evidence has an important role to play in informing public engagement and consultation. It is noted that the evidence base should also be referred to in the Data Protection Impact Assessment (DPIA).

3.1 **All business cases** (and hence templates) completed by policing bodies **should require the inclusion of a basic assessment of the evidence base, drawing on available research** (and learning from other jurisdictions) **and including both benefits and dis-benefits.** The level of risk (see chapter 8) should determine the level of evidence gathering required. For medium-risk projects (or projects with high value investment) an evidence review should be required. For all high-risk projects a more thorough evidence review (ideally with external input or review) should be required, or indeed in some cases the generation of further independent research may be necessary (particularly if the evidence base is lacking) to inform decision making regarding adoption.

3.2 Policing bodies should also **draw together the evidence base to support consultation and public engagement work**. A balanced, clear and succinct public facing summary of the existing research and other evidence (acknowledging any limitations and gaps in knowledge) should be developed (with input from independent external stakeholders, particularly for high-risk projects) in order to be shared during public engagement and consultation exercises.

Innovation: Scientific evidence about what works best should be central to innovation and shaping police practices. Using a combination of best practice research evidence, industry knowledge and experience, and taking into account the experience of members of the public (including victims of crime and others involved in the criminal justice system) is key in order to make informed decisions on the adoption of emerging technology in policing. In order to support innovation, if pilots are being developed, consideration should be given to doing this in collaboration with academia, industry and other stakeholders. If industry are developing pilots they should engage with the research community in order to build evidence-based solutions.

Evaluation: It is important to consider whether a pilot (rather than full roll-out) is the most suitable first step. Furthermore, it is crucial to consider whether an evaluation is needed, and how it can be in place ahead of changes happening. Evaluations may be focused on a pilot or full roll-out, and on either the implementation (process evaluation) or the impact of new technologies (outcome evaluation). Support in commissioning evaluations should be sought prior to technological adoption and baseline measurements must be gathered.

3.3 **The decision about whether an evaluation of the impact of new technologies in policing is needed should be informed by the level of risk and the existing evidence base.** For existing systems with a history of safe operation an evaluation would only be necessary if they undergo significant changes in their design or intended purpose. For high-risk projects an evaluation should be carried out and commenced at the earliest point possible prior to development, acquisition or adoption of a new tool, means or method of policing. In relation to commissioning evaluations, third party support (e.g. through SIPR) should be sought very early on and the evaluation should include baseline impact measurements. Steps should be taken to safeguard the quality and independence of the evaluation e.g. establishing a Research Advisory Group and peer reviewing of reports.

3.4 In addition to accessing learning and research on best practice in the use of emerging technologies from other jurisdictions (including from other police forces) to inform decision making (e.g. business cases and sixth case assessment) and design processes,

opportunities for knowledge exchange (where possible in open fora) should continue to be maximised by policing bodies throughout implementation and ongoing review.

3.5 The existing knowledge base and **suggestions for further research identified by Connon et al. (2023) should be reviewed** by policing bodies and key stakeholders in order to **prioritise areas for further research**. An assessment should be undertaken of the level strategic importance, level of risk, and potential value of the research in order to guide decision making on which areas should be prioritised for funding by various partners (Scottish Government, Police Scotland, Scottish Police Authority, the Scottish Institute for Policing Research etc.). In addition, suggestions should be shared with SIPR and wider the academic community who are keen to undertake independent research and leverage external funding e.g. from research councils.

4. Legal frameworks

This chapter covers legal frameworks (human rights, equalities, data protection and law of evidence); impacts on individuals' rights, processes (including impact assessments) and procedures (including digital evidence gathering); lessons learned, good practices and legislative gaps. It is based on both the report of the first workstream of the IAG (Daly et al. 2023) and the work of the commissioned research report (Connon et al., 2023). As mentioned above, our analysis is based on current legislative frameworks in force at the time of writing and excludes consideration of UK Government proposals for legislative reform, in particular the Data Protection and Digital Information Bill and Bill of Rights Bill. We consider EU data protection standards contained both in the GDPR and Law Enforcement Directive, as currently implemented in UK law, to be best practice and ought to continue to be adhered to by authorities in Scotland even if they are no longer legislative requirements.

Background

As outlined by Daly et al. (2023), with the rapid acceleration of technological advances over the past 10 years policing bodies in Scotland have expressed a need to increase their technological capabilities in order to fulfil their statutory role of prevention, detection and apprehension of crime. Over the past five years Police Scotland have made a significant commitment in Policing 2026 and its implementation plan, to engage in digital policing and focus on their approach to cybercrime, developed in their Cyber Strategy. This has resulted in greater engagement with technology internally and significant external engagement with stakeholders and regulatory bodies. During this period Police Scotland have been challenged and criticised by parliamentary committees, national human rights institutions, statutory inspection bodies and stakeholders with regard to its implementation of human rights standards to guide policing. It is in this context that the IAG was formed and recently we have seen the establishment of the independent Scottish Biometrics Commissioner (SBC), 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.

Legal frameworks:

Connon et al. (2023) detail various legal considerations associated with the adoption of emerging technologies in policing. In their report they have identified relevant UK case law (in Appendix 3), International C case law (Appendix 4) and key provisions of significant legislation (and the technologies to which they may apply, Appendix 5). The latter also cites relevant case law addressing each legislative provision and is a useful tool against which to evaluate the legal issues/considerations presented by a specific piece of emerging technology. Connon et al.'s work on law of evidence is covered later but firstly information from Daly et al.'s (2023) report is used to outline Human Rights, Equalities, Data Protection and Biometrics considerations, supplemented by information from Connon et al.'s report.

Human rights:

As covered by Daly et al. (2023), as part of the UK, which is a signatory of the European Convention on Human Rights (ECHR), and as per the Scotland Act 1998, Scottish public entities bear the primary duty to promote, protect and fulfil human rights as specified. States have a positive obligation to protect against discrimination and promote equality. The ECHR has some domestic effect in the UK via the Human Rights Act 1998 and section 6 makes it unlawful for a public authority to act (or fail to act) in a way which is incompatible with a Convention right. Scottish Government and policing bodies should place human rights at the core of how emerging technologies are used in policing. Key ECHR rights engaged by the use of emerging technologies are listed (Daly et al., 2023: 16) but include e.g. right to liberty and security; respect for private and family life, home and correspondence; freedom of expression; freedom of assembly and association; protection from discrimination in respect of these rights and freedoms.

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. The impact and the 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 is an emerging body of human rights jurisprudence on the development and use of digital technologies, emphasising their need to be centred within a human rights framework, which 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. Human Rights impacts explored by Connon et al. (2023) are covered below.

Equality Act 2010:

As explored by Daly et al. (2023), The Equality and Human Rights Commission published guidance on the Equality Act 2010 (EA 2010), which protects individuals from discrimination, victimisation and harassment because of protected characteristics (age, disability, gender reassignment, marriage and civil partnership, pregnancy and maternity, race, religion or belief, sex and sexual orientation) and supports progress on equality. The EA 2010 prohibits direct and indirect discrimination, discrimination arising from disability, failure to make reasonable adjustments for disabled people, harassment and victimisation.

The Public Sector Equality Duty (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 carrying out their activities (see section 149 of EA 2010). Not ensuring consideration of equality can lead to unlawful discrimination, greater inequality and worse outcomes for particular groups of people in our communities. The general duty requires equality considerations be built into the design of policies and practices and the delivery of services, and for these to be kept under review. The EHRC has issued guidance on the PSED for Scottish public bodies.

Scottish Minsters, Police Scotland and the Scottish Police Authority have legal obligations under PSED as service providers and employers. Of note 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 (regulation 5 of EA 2020 (Specific Duties) (Scotland) Regulations 2012 as amended). Chapter 6 of the technical guidance on the Public Sector Equality Duty: Scotland describes what's required from public bodies in carrying out an equality impact assessment. It sets out a number of steps including assessing 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; taking account of results in developing proposals and ensuring due regard when making decisions about the policy and its implementation, documenting decisions, publishing results and monitoring the actual impact of the policy.

There is also a specific duty requirement to consider the use of equality award criteria and conditions in relation to public procurement and the EHRC has published procurement guidance for Scottish public authorities in order to assist with compliance. On a practical level Police Scotland need to make sure they have systems and processes in place to gather and use equality data of employees in order to meet requirements of EA 2020 (Specific Duties) (Scotland) Regs 2012 (as amended); and collate and use equality data of service users as a means of demonstrating compliance with section 149 of EA 2010. EHRC have published guidance on Artificial intelligence: meeting the Public Sector Equality Duty (PSED).[1]

Connon et al. (2023) point out that where emerging technology is to be deployed in a context involving children, steps will have to be taken to ensure compliance with the United Nations Convention on the rights of the Child. They argue that the implementation of UNCRC into domestic law has consequences and further research is required to explore how children's rights may be affected by the implementation of emerging technologies in the context of policing and how they can be appropriately secured.

Data protection:

As described by Daly et al. (2023), UK law at the time of writing reflects EU standards in data protection ('UK GDPR'), given the Data Protection Act 2018, which implement recent reforms to EU law in this area including the General Data Protection Regulation and Law enforcement Directive. Therefore, law enforcement authorities in Scotland are subject to UK data protection law which incorporates UK GDPR and the Data Protection Act (DPA 2018). Which data protection regime applies depends on the primary purpose of the processing and nature of the body carrying it out.

Part 3 of the DPA 2018 applies to competent authorities processing personal data for law enforcement purposes. Law enforcement purposes are defined under section 31 of the DPA 2018. The main responsibilities for authorities processing personal data of law enforcement purposes are set out in chapter 2, Part 3 of the DPA 2018, and for general processing, in Article 5 of the UK GDPR. Data protection law is regulated by the UK Information Commissioner's Office (ICO).

The legislation expressly prohibits the processing of data for non-law enforcement purposes unless it is authorised by law. As Connon et al. (2023) point out police are often engaged in

[1] Artificial intelligence: meeting the Public Sector Equality Duty (PSED) | Equality and Human Rights Commission (equalityhumanrights.com)

activities considerably beyond the definition of law enforcement purposes and therefore Police Scotland would need to ensure there is an appropriate authorisation in law for processing. This is likely to be important in the interaction between private sector organisations who may be involved in developing technologies or providing services as there may be restrictions e.g. on the use of data for development of technology or the sharing of data with third parties.

Sensitive data/special category data:

Both data protection regimes provide additional protections for what is known as sensitive personal data or special category data. Sensitive processing is defined in section 35(8) of the DPA 2018 is defined in section 35(8) of the DPA 2018 and special category data is defined in Article 9 UK GDPR. Both sensitive processing and special category data includes biometric data where used for the purpose of uniquely identifying an individual.

When undertaking 'sensitive processing' in order to comply with the first principle the processing must be based either on the *consent* of the data subject or policing bodies must be able to demonstrate that the processing is *strictly necessary* for law enforcement purpose and based on a Schedule 8 DPA 2018 condition. The standards for valid consent (ICO website definition) under data protection law are high and difficult to obtain in practice, therefore in most cases competent authorities (ICO website definition) processing sensitive data must be able to demonstrate that the processing is **strictly necessary** (relates to a pressing need and cannot reasonably be achieved through less intrusive means) and be able to satisfy one of the conditions (ICO website definition) in Schedule 8 of the DPA 2018. Competent authorities also need to ensure there is an appropriate policy document (ICO website definition) in place.

Data protection impact assessment:

As outlined by Daly et al. (2023), DPIA (ICO website definition) must be carried out by controllers before they process personal data, when the processing is likely to result in a high risk to the rights and freedoms of individuals. Processing that is likely to result in a high risk includes for example: systematic and extensive processing activities (including profiling) and where decisions that have legal effects or significant effects on individuals; large scale processing of special categories of data or personal data relating to criminal convictions or offences; using new technologies (e.g. surveillance systems).

It is highly likely that a DPIA will be required for proposals that involve the use of new technologies by competent authorities. Even where a DPIA is not required by law it is good practice to carry out a DPIA for all new processing and an effective DPIA will allow controllers to identify and fix problems at an early stage.

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. As Connon et al. (2023) argue, and as the ICO recommends in its Guidance, DPIAs and data protection policies should be kept under regular review to ensure they capture the development and use of emerging technologies and DPIAs should be carried out prior to any development but then revised as it progresses from trial to deployment.

ICO guidance sets out that data protection by design starts at the initial phase of any system, service, product, or process. This means that policing bodies must, prior to implementing any intended processing activities, consider the risks that these may pose to individuals, and the possible measures available to ensure compliance with the data protection principles and protect individual rights.

Data protection by design and default:

Under Art 25 UK GDPR and Part 3 of DPA (Section 57 (Link to legislation.gov)), controllers have a general obligation to implement appropriate technical and organisational measures to show that they have considered and integrated - i.e. 'baked in' - the principles of data protection into processing activities, from the design stage right through the lifecycle. ICO guidance sets out that data protection by design starts at the initial phase of any system, service, product, or process. This means that policing bodies must, prior to implementing any intended processing activities, consider the risks that these may pose to individuals, and the possible measures available to ensure compliance with the data protection principles and protect individual rights. The ICO published guidance on privacy by design and default within the Guide to the UK GDPR.

Automated decision making:

As Daly et al. (2023) describe, under sections 49 and 50 Part 3 DPA 2018 and Art 22 UK GDPR, individuals have the right not to be subject to a decision that is based solely on automated processing which has a legal or similarly significant effect on them unless the conditions set out in the legislation are met. Where the processing is for law enforcement purposes to comply with Section 49 DPA 2018 the decision must be required or authorised by law and the safeguards set out Section 50 of the DPA 2018 must be met.

Under UK GDPR where Article 22 is engaged the processing must be necessary to fulfil a contract, be authorised by law and subject to the safeguards set out in domestic law or based on the individual's explicit consent. In both regimes individuals retain the right to obtain human intervention; express their point of view; 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). As Connon et al. (2023) argue and as the ICO notes in its guidance on AI and data protection (ICO website definition) artificial intelligence processes pose challenges with accountability and transparency of operations and therefore it will be necessary to ensure that appropriate procedures are in place to ensure consideration is given to whether there is ambiguity in the quality, reliability, or transparency in how data is being processed by automated means, that controllers are able to identify when an automated decision is taking place, that data protection legislation can be complied with and that individuals are able to access their rights under Section 49 and 50 DPA 2018 and Article 22 UK GDPR .

Artificial intelligence guidance:
The ICO has developed best practice guidance on AI and data protection (ICO website) for controllers to take into account in processing of personal information that involves AI. It sets out the interpretation of data protection law as it applies to AI systems that process personal data and contains advice on how to interpret relevant law as applies to AI and provides recommendations on organisational and technical measures to mitigate risks. Where a controller is planning to use AI and undertaking data analytics the ICO

recommends its Toolkit for organisations considering using data analytics at the outset to recognise risks to rights and freedoms.

Biometrics:

The Scottish Biometrics Commissioner Act 2020 defines, for criminal justice and policing purposes in Scotland, biometrics data and sets up an independent public body for promoting and supporting the legal, ethical and effective acquisition, retention, use and destruction of biometric data.

It should be noted that the definition of biometric data in the SBC Act differs from the definition of biometric data in UK data protection law and includes for example photographs[2]. The use of biometrics is supplemented by a number of other legal frameworks (Daly et al., 2023: 25). The Scottish Biometrics Code of Practice came into force on the 16 November 2022. The Code of Practice provides a high-level summary of 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.

The law of evidence:

Improperly obtained evidence:
As detailed by Connon et al. (2023) evidence may be obtained in a number of ways including search of persons, premises, personal property, taking of samples and use of surveillance technologies. For evidence to be considered 'legally obtained' it must comply with the rules of evidence and if it does not do so it is considered to have been obtained improperly. If obtained improperly its admissibility can be questioned, and the common law rule on admissibility of improperly obtained evidence is a balancing exercise between the interest of the citizen to be protected from illegal invasion of liberties and the interest of the state to secure evidence bearing on the commission of crime and necessary to enable justice to be done.

It has been recognised that such evidence should not be withheld from court on any merely formal or technical ground.[3] Where information is improperly obtained, in addition to admissibility, the most likely grounds of challenge are Article 5 (Right to Liberty and Security), Article 6 (Right to a Fair Trial), and Article 8 (Right to Private and Family Life) of the European Convention of Human Rights.[4]

Beyond common law principles, there are statutory forms of regulation that impact on whether or not intelligence or evidence has been legally obtained: Criminal Procedure (Sc) Act 1995, Regulation of Investigatory Powers (Scotland) Act 2000, Police Act 1997, Investigatory Powers Act 2016 as well as compliance with the National Assessment Framework for Biometric Data Outcomes and the Scottish Biometric Commissioners' Code

[2] Scottish Biometrics Commissioner | What Are Biometrics? | Scottish Biometrics Commissioner
[3] Lawrie v Muir 1950 JC 19 at 26.
[4] See Diego Quiroz, SHRC, Human Rights and New Technology in Policing Issue Paper for the IAG, May 2021. Available: human-rights-and-emerging-technologies-in-policing-issue-paper-vfinalforonline.pdf (scottishhumanrights.com)

of Conduct.[5] The use of emerging technologies is likely to challenge the boundaries of these legislative measures.[6] Examples are provided in Connon et al. (2023) but it is noted that the SBC Code of Practice is likely to address these ambiguities surrounding biometric data at least.

Following some controversy, the Police, Crime, Sentencing & Courts Act 2022 introduced a system of regulation specifically focused on authorisation of the extraction of information from electronic devices[7]. As Connon et al. (2023: 62) outline in more detail these provisions should offer clarity on the process to be followed, the limitations on the extraction of information, the purposes and restrictions on the scope of these purposes and must adhere to a forthcoming code of practice.

Disclosure of evidence:
Part 6 of the Criminal Justice & Licensing (Sc) Act 2010 set out the rules of disclosure which mean that an investigating agency must provide all information relevant to a case for or against an accused that was obtained in the course of investigating. A failure to disclose information to the defence at an early stage could result in a case being challenged on the basis of prejudicial effect of the information not being made available. This is likely to present a problem as automated decision-making systems, AI and algorithms become more embedded in policing practice as the transparency of such systems is problematic.[8]

At an international level, Connon et al. (2023) outline measures being developed that seek to facilitate the disclosure of electronic evidence, e.g. a Protocol to the Cybercrime Convention[9], which seeks to enhance cooperation between states to ensure offences recognised by the cybercrime convention can be effectively investigated and prosecuted. Although the UK is not yet a signatory, the framework facilitates lawful basis for exchange of evidence which is likely to impact transparency, accountability and trust in the police.

Impacts

Impact on rights and freedoms:

As outlined in Daly et al. (2023) Human rights impacts will depend on the type of technology used, the use case, and must be examined in context and take account of impacts at multiple levels (individual, community or society-wide). In some cases it is impossible to anticipate the full impact of police use of technology on human rights and harm may be difficult to quantify, particular as it may continue into the future (e.g. if personal data is shared or sold). It is important to ensure that any private actors involved comply with

[5] Scottish Biometrics Commissioner: National Assessment Framework for biometric data outcomes, January 2022 and s7, Scottish Biometrics Commissioner Act 2020. asp 8.
[6] Steven J. Murdoch, Daniel Seng, Burkhard Schafer and Stephen Mason, The sources and characteristics of electronic evidence and artificial intelligence, Chapter 1, in Stephen Mason and Daniel Seng (eds) Electronic Evidence and Electronic Signatures, (5th ed, 2021). pp1-50.
[7] See the recommendations of the Information Commissioner's Office (2021) Mobile Phone Data Extraction by Police Scotland, Investigative Report, June 2021. Available at: ico-investigation-mpe-scotland-202106.pdf [Accessed 16 April 2022]. (Discussed at section X below). Section 37-44, The Police, Crime, Sentencing & Courts Act 2022.
[8] Quezada-Tavárez, K. Plixavra Vogiatzoglou, Sofie Royer, Legal challenges in bringing AI evidence to the criminal courtroom, (2021) Vol. 12(4) New Journal of European Criminal Law 2021, 531–551. DOI: 10.1177/20322844211057019.
[9] Second Additional Protocol to the Convention on Cybercrime on enhanced cooperation and disclosure of electronic evidence Strasbourg, 12.V.2022

applicable laws and respect human rights. Depending on whether they are controllers or processors they will have different obligations under data protection law and different governance is required to ensure compliance. Some concerns include the amplification of discrimination resulting from digital technologies (e.g. AI and machine learning systems) which are dependent on historic data which may be incomplete or contain bias. However, with regulation and governance of the design and development of new technologies (particularly AI) they may be used to advance, rather than put at risk, equality and human rights.

Impacts may occur at a societal level, e.g. risks to democratic freedoms (impacting articles 9-11 of ECHR) can arise from widespread use of surveillance tools and AI-enabled technologies by police. For example, 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 and any deployment must be in compliance with data protection law. The proportionality principle requires any surveillance measure used should be the least invasive option. UK surveillance laws applicable to certain bulk surveillance practices, must respect these principles.

Facial recognition technologies employed at large events therefore raise human rights (proportionality) concerns as well as being potentially discriminatory. The issues have been considered in the UK context in the Bridges/South Wales Police case and the ICO in its opinions on live facial recognition technology by law enforcement in public places (ICO website) in 2019 and 2021 the use of live facial recognition technology in public places. (ICO website) Risks also include discrimination, particularly to African descendants and other minorities, women and persons with disability, given literature on algorithmic error rate in facial recognition technologies. Although live facial recognition is not currently used by Police Scotland, non-live versions may still exhibit discriminatory biases. Important steps are being taken to clarify legal frameworks governing biometric data through the Scottish Biometrics Commission's Code of Practice covering acquisition, retention, use and destruction of biometric data for criminal justice and police purposes. However, given the issues identified and growing unease with live facial recognition internationally, including outright bans on police use, we would need to see strong justifications for its use in order to establish 'benefits' and for an array of concerns to be adequately addressed.

Databases: As Connon et al. (2023) point out, in addition to many concerns about negative impacts on human rights, it is possible that technologies may support human rights protections (e.g access to real time translation would support the right to a fair trial by providing information promptly on the nature of the accusation). Connon et al. (2023) provide some examples of legal challenges to the deployment of new technologies, often framed in terms of the Article 8 right to privacy.[10] For example, poor governance of the use of databases has been challenged on the bases that they breach data protection law and the inclusion of personal data on them is an infringement of Article 8 ECHR. For detail of these challenges see Connon et al. (2023: 71), which relate to whether data should be retained, for how long and at what point it should be deleted.

[10] European Court of Human Rights, Factsheet: New Technologies. April 2022. Available: FS_New_technologies_ENG (coe.int).

Connon et al. (2023) note that *biometric identification systems* are likely to be operationalised through the use of a database of some kind. They point out that although failure to comply with the SBC CoP will not in itself give rise to grounds for legal action, compliance with the code must be taken into account in deciding whether evidence has been improperly obtained. Furthermore, data protection law must be complied with and non-compliance will face regulatory action from the ICO. They also note that the collection and use of biometric data in the form of facial recognition has faced significant judicial attention via the Bridges/South Wales Police case in the English and Welsh Courts (for details see Connon et al. 2023, Appendix 3 and section 3.5.2). There were criticisms of the governance framework used by the police force, the data protection impact assessment had failed to grasp risk to human rights and freedoms of data subjects and had not taken steps to evaluate its potential discriminatory impacts before, during and after the trial. The Bridges decision recognised the value of the Code of Practice issued by the Secretary of State and guidance produced by the Surveillance Camera Commissioner in 2019 on police use of AFR technology with surveillance camera technology but were critical of the generic nature of each and were concerned about a lack of specific policies regarding inclusion of individuals on watch lists or justification for selecting particular locations for the use of AFR. It is worth noting that the code of Practice of the Biometric and Surveillance Camera Commissioner relates to England and Wales working across borders will require compliance with that framework as well as those in Scotland.

The use of emerging technology for the purposes of *electronic surveillance and monitoring* is subject to regulatory frameworks set out in various investigatory powers acts (Regulation of Investigatory Powers Act 2000, RIP Scotland Act 2000) and data protection law (Connon et al. 2023: 75), where with failure to comply there is potential for a breach of human rights and it may impact on admissibility of evidence. The legislation distinguishes between 'directed surveillance' (covert surveillance that is not intrusive and relates to obtaining private information about a person who may or may not be the focus of an investigation) and 'intrusive surveillance' (covert surveillance that focuses on residential premises or private vehicle where the surveillance is carried out by an individual but also by means of a surveillance device). Significantly, surveillance may be considered intrusive if remote surveillance technology can achieve sufficiently reliable quality of data. Directed surveillance can be authorised on the grounds it is necessary to prevent or detect crime or prevent disorder, in the interests of public safety or protection of public health, whilst intrusive surveillance should only be authorised where it is considered necessary to prevent or detect *serious* crime. Importantly, if a new technology is developed that would obtain the same data as an already available means the question would be raised whether it is needed at all because in assessing whether intrusive surveillance is necessary and proportionate consideration must be given as to whether the same information could be obtained by other means.

In relation to the regulation of automated decision making, Connon et al. (2023) point out that where it is necessary and proportionate for the prevention, investigation and prosecution of criminal offences there is an exception to the provision that an individual should not be the subject of a solely automated decision-making process (see sections 49 and 50 of DPA 2018 and Article 22 of UK GDPR). The 2017 Council of Europe study on the human rights implications of automated data processing techniques[11] highlighted that in

[11] Council of Europe (2017) Study on the Human Rights Dimensions of Automated Data Processing Techniques (in particular Algorithms) and Possible Regulatory Implications. DGI(2017)12.

addition to design flaws in algorithms datasets may contain bias that is replicated or magnified by the algorithm (Završnik, 2021) and there are further challenges with human interpretation of the algorithm. There are clear concerns around automated decision making and AI (Binns, 2022), including limited ability to achieve transparency in how data is processed given opacity of algorithms).

Connon et al. (2023) highlight that the UK Office for AI have issued guidelines for the procurement of AI in government (2020) and an ethics, transparency and accountability framework (2021) which includes an algorithmic transparency template but these are not legally binding (in stark contrast to the Canadian system). The Justice and Home Affairs committee of the House of Lords have raised concerns that there is no central register of AI technologies in the UK, which is problematic for transparency and accountability and they argue there should be a 'duty of candour' on police to ensure transparency in the use of AI enabled technologies. Algorithms have the potential to exacerbate and escalate biases and JHAC were concerned there were not scientific or ethical standards an AI tool should meet before it can be used in the criminal justice sphere. It is noted that the Alan Turning Institute is now leading a project seeking to draft global technical standards.[12] International developments to enhance ethical approaches to the use of algorithms include OECD Principles of Artificial Intelligence.[13] G20 AI Principles and UNESCO adopted a Recommendation on the Ethics of AI.[14] Finally, the Council of Europe are in the process of developing a convention on the use of AI that is due to be completed in 2023.[15][16]

Data protection and equality impact assessments:

Police Scotland report that since 2018 they have worked to make the use of DPIA's systemic for all new or updated processing, including the introduction of new technologies. They emphasise that their impact assessment procedures are aligned, e.g. DPIA and Equality and Human Rights Impact Assessments (EQHRIA) are in concert with each other. The two frameworks are used to guide the design, build and implementation of technologies and processing by working with a range of specialists to discuss risks and identify solutions. Examples have been provided of where changes have been made in order to ensure compliance, for more details see Daly et al. (2023: 29).

It has been suggested that Police Scotland may wish to consider undertaking Children's Rights and Wellbeing Impact Assessments (CRWIAs) alongside DPIAs and EQHRIAs as a way of further embedding a human rights based approach. In relation to equality impacts, it is noted that technologies based on predictive analytics which leverage data and other technologies to monitor and assess individuals, communities and or specific locations can target particular protected characteristic groups over others e.g. 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. EQHRIA processes must help identify potential discrimination, consider possible impacts on people

[12] UK Government, New UK initiative to shape global standards for Artificial Intelligence - GOV.UK (www.gov.uk), Press Release.
[13] OECD Principles on Artificial Intelligence May 2019: Artificial intelligence - OECD
[14] G20 AI Principles, June 2019: G20 AI Principles - OECD.AI; UNESCo Recommendation on Ethics of AI. November 2021. Available: Recommendation on the ethics of artificial intelligence (unesco.org)
[15] Council of Europe's Work in progress (coe.int)
[16] Council of Europe, Consultative Committee of the Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data. Guidelines on Facial Recognition, 28 January 2021, T-PD(2020)03rev4.

with protected characteristics (and any inequalities, barriers or specific needs) and opportunities to advance equality when designing, commissioning or using new technologies. This is reinforced by data protection law, according to which controllers must identify and assess all potential risks to rights and freedoms including the risk of discrimination and identify and implement measures to mitigate and manage these risks (section 65 DPA 2018 and Article 35, UK GDPR)

Processes for establishing legal basis:

As detailed in Daly et al. (2023) Police Scotland have explained that they primarily use the established frameworks of a DPIA and EQHRIA to establish, define and document the legal basis it relies on for the use of new technology. Lawfulness is at the heart of the DPIA, addressing the legislative requirement that processing must be both lawful and fair. Police Scotland assert that the DPIA and EQHRIA frameworks allow them to design the necessary legislative and regulatory compliance into the new technology. An initial *indicative* legal basis is tested and developed given input from a number of internal and external actors and they distinguish between the purpose of processing and the manner of processing (with the latter less clear at the outset). Although the Police and Fire Reform Scotland Act forms a backbone to many police activities the legislative provisions that may be elide upon as legal bases are many and lengthy. Learning from Cyber Kiosks (also known as digital triage devices) has been drawn on and in recent examples such use of BWV by armed officers Police Scotland developed a Code of Practice (Police Scotland website link) and the EqHRIA and DPIAs are treated as live documents - see Daly (2023: 33) for more information.

Wider views beyond Police Scotland consider that there is a lack of clarity or even insufficient legislation in Scotland to facilitate and justify police use of emerging technologies for certain purposes. For example, there was significant controversy and disagreement among stakeholders about whether there was an appropriate basis for Police Scotland to use Cyber Kiosks. Whilst Police Scotland claimed the legal basis exists, others such as SHRC were of the view that there is an insufficiently clear legal basis for this. 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).

It is noted that further controversies may arise given the lack of clear and explicit legal framework and policy guidance for other technologies such as: facial recognition, drones, body worn cameras, data driven analysis, AI systems and the use of personal data collected and processed by these technologies. The ICO has produced guidance on a number of these issues (live facial recognition use by law enforcement (ICO website) and more generally in public places (ICO website), the use of video surveillance (ICO website), and on AI and data protection (ICO website)). and the Ryder Review (Independent Review of the governance of biometric data in England and Wales) recommended a legally binding code of practice for live facial recognition should be formulated.

Data sharing by police and other agencies also gives rise to concern and may negatively impact on human rights. Although there is insufficient knowledge of the extent of data sharing in Scotland, there have been reports of disabled people being photographed by

English police forces at an Extinction Rebellion protest and their details passed to the Department of Work and Pensions. However, human rights standards prohibit collection of personal data to intimidate participants in a protest. As with any processing of personal data, data can only be shared lawfully by the Police if there is a clear basis in law and the sharing would not result in an infringement of any other law (including Human Rights law).

Given the police's role in investigating allegations of criminal behaviour there are 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 and data protection in the blanket retention of biometric data: DNA profiles (cellular samples and fingerprints and custody photographs) and bulk surveillance of the public. The SBC Code of Practice should be referred to.

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 highlighted the proliferation of AI tools by police forces without proper oversight. It acknowledged the opportunity of AI to help prevent crime but stressed the risk to exacerbating discrimination and highlighted that '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.'

The 2022 UK Government policy paper, Establishing a pro-innovation approach to regulating AI, however considers that any regulatory activity should be directed towards AI presenting 'real, identifiable, unacceptable levels of risk', but for now does not consider legislation to be necessary; instead it plans to introduce a set of non-statutory cross-sectoral principles on AI. The Scottish Government launched its own AI Strategy in 2021, in which it set out its vision to become 'a leader in the development and use of trustworthy, ethical and inclusive AI' but there is no mention of police use of AI in the paper. The SG 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, but again policing is not mentioned in this strategy.

The response to the IAG public consultation (call for evidence) 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 legal assessment framework would likely mitigate legal, jurisdictional and operational challenges from transpiring and reduce risks to public trust, feelings of oppression and surveillance, and discrimination. The need to engage critical assessment or external consultation was also raised. It was suggested that an ethical and legal assessment framework should embrace an equality and human rights-based approach to understand impacts on individuals (including witnesses, victims, suspects, member of the public and protected characteristic groups) and provide strong and unbiased evidence that the proposed technology is non-discriminatory and will not entrench existing inequalities and explain why it is necessary ad proportionate, largely reflecting and reinforcing existing requirements under legislation including data protection.

Procedures and digital evidence gathering:

In considering policing procedures and digital evidence gathering 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, hope and correspondence). Smartphone devices which may be examined by police are incomparable to paper documents or more basic computers given they store, transmit, communicate large amounts of data, some of which is jointly owned or belonging to others and can be obtained without their consent. The information found on a mobile device may provide profound insights into an individual's behaviour, beliefs, and emotional state. Evidence extracted from a digital device may be critical to criminal investigations but a device should only be reviewed, and information extracted, where it represents a reasonable line of enquiry. There is also an issue with the use of technology to extract information, including bypassing security protocols and a robust approach to regulation and scrutiny is required.

In 2021 the ICO published the findings of an investigation into the use of Mobile Phone Extraction in Scotland. Six recommendations for Police Scotland and one recommendation for COPFS and SPA were made. These included recommendations on establishing controllership, DPIAs, transparency, retention, adherence to forensic standards and working with UK partners to implement the new powers under the Police Crime, Sentencing and Courts Act 2022 (see sections 37-33) and recently published Code of Practice which applies in Scotland.

The Bridges case, currently example of English case law and not binding in Scotland, on facial recognition emphasised that clear guidance on the use of technology and who could be targeted were issues of legality, and in the absence of such a guidance a finding that interferences was in accordance with the law was not sound. Scotland is set to become a forerunner in the regulation of biometric data use by police as the SBC draft Code of Practice 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. This is a positive step and its implementation and evaluation should inform how procedures and evidence gathering (even beyond biometric data) can be improved to reflect best practice in human rights, equalities and data protection.

It should also be noted that a fully digitised justice system is a key objective outlined in the Digital Strategy for Justice in Scotland and this includes a focus on providing digital recording of evidence, reports and a secure digital platform to secure all information relevant to a case.

Drones and evidence case study:

Drones (RPAS) 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, potentially using ANPR or facial recognition technologies). Legal issues will vary depending on the deployment context. There is a need for robust impact assessments and the use of drones is subject to a number of legal requirements, including compliance with human rights, equalities and data protection requirements and Civil Aviation authority regulations. As

drones will likely capture sensitive personal data there is a requirement to demonstrate that no less intrusive means are suitable. For drones the risk of 'collateral intrusion' is likely to be more extensive than for other means so demonstrating this necessity is important in an impact assessment. Deployment at public protests would require detailed justification as political belief constitutes sensitive personal data.

There is detailed guidance from the ICO on the use of drones under UKGDPR (although this does not cover Part 3 law enforcement processing) and measures required may include the prohibition of continuous recording, restriction of recording at lower altitudes, restricted field of vision or other means. A particular challenge is the requirement to provide notification of drone operation in an area. Privacy by design (e.g. encrypting any locally stored data) is required. The use of drones has not seen significant challenge in courts in Scotland but the Bridges case is of relevance. Internationally the use of drones is often considered under prior legal frameworks around police helicopter surveillance for example but a number of states in the US have prohibited the use of drones for police or other surveillance on constitutional grounds.

Lessons learned, good practices & legislative gaps:

Daly et al. (2023: 48-60) cover four case studies highlighting **lessons learned from a Scottish perspective** relating to: cyber kiosks, mobile working, BWV, and drones. Although much of this is covered in the next chapter, some of the implications from a legal standpoint are briefly outlined here. As previously alluded to the legal basis of Police Scotland's use of *Digital Triage Devices* had been called into question. Open Rights Group, Privacy International and the Scottish Human Rights Commission were among the stakeholders who believed there was a lack of a clear legal basis for their use. The Justice Sub-Committee on Policing Report (2021)[17] emphasised the need to undertake necessary assessments, confirm the legal basis and to consult relevant stakeholders prior to making a decision.

When it comes to legal considerations regarding emerging technologies such as *drones* it is clear that the policing context in which drones are deployed (e.g. missing persons versus surveillance of a large public event) impacts on the extent to which legal issues such as right to privacy would be engaged (see previous section). Daly et al. (2023) cite the deployment of BWV devices to armed police officers in Scotland prior the COP26 conference in Glasgow in 2021 as an example of improvements made to mitigate against potential privacy and third-party concerns. Police Scotland completed full EqHRIA and DPIAs (these are treated as live documents to be reviewed and updated annually to reflect changes in legislation, policy and technology) and developed and published a detailed Code of Practice outlining how BWV is to be used in armed policing.

Daly et al. (2023: 60-68) also draws out some **insights from other jurisdictions**. For example, equivalence has been drawn between Article 8 ECHR and section 8 of the Canadian charter of rights and freedoms. The Canadian Supreme Court has a growing body of jurisprudence distinguishing between traditional searches and searches of devices and cyber space. The case of Fearon determined that the search of a mobile phone was

[17] Police Scotland's use of remote piloted aircraft systems and body worn video cameras | Scottish Parliament

not an inevitable breach of privacy. This highlights that privacy safeguards or modifications (e.g. tailoring the nature and extent of the search around purpose it is being lawfully conducted for) can be used to preserve human rights of the target of the search. As Daly et al. (2023) point out the officer deciding to search must be capable of compressively appreciating the human rights being engaged at the time and therefore 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.

There is some controversy about the clarity and ambiguity (or lack thereof) in the interpretation of the legal opinion obtained by Police Scotland on the legal basis of Cyber Kiosks which cites the Canadian cases. Daly et al. (2023) argue that it was concerning that Police Scotland's assertion that the opinion was clear and unambiguous was a narrow interpretation of it and obscured the context of the advice. Indeed, the author made several recommendations and identified legislation and a code of practice as best practice. Whilst Canadian jurisprudence has acknowledged e.g. that the profiling of suspects on the basis of their ethnicity is unlawful, a comprehensive framework covering all aspects of emerging technologies does not yet exist.

Daly et al. (2023) highlight that the Privacy Commissioner of New Zealand consider their legal framework to be adequate to address the field of biometric deployments (including facial recognition for identification purposes), though they are considering whether their Privacy Act 2020 should be supplemented by a code of practice. Crucially, given the interdependent nature of technological advance, it is worth noting that the Privacy Act applies to both public and private bodies like data protection law in the UK. Also of interest is that NZ immigration legislation limits the use of AI in decision making, requiring the prescription of personal responsibility to decisions. Many NZ government agencies have voluntarily subscribed to an Algorithm Charter that provides a legal framework for Artificial intelligence related products and services.

Daly et al. (2023) also highlight international law and norms, including at an advisory level respect for fundamental rights derived from the ratification of UN Treaties and Committees. Key principles can be distilled from International l29aw e.g. Article 17 ICCPR. The Council of Europe and its delegate bodies also have detailed legal frameworks, some of which are biding in law. Finally, international non-governmental organisations such as Amnesty International have published guidance relevant to policing. Other international standards that should be given due consideration include the jurisprudence and general comments from human rights bodies to which the UK is a member (e.g. UN guiding principles on use of personal and non-personal information, on business and human rights). As Daly et al. (2023) argue there is a legitimate expectation that private actors (both controllers and processors e.g. those developing technologies which may be used by police) should comply with all applicable laws and respect human rights and data protection law. As Daly et al. (2023) point out, the European Parliament supported the European Commission's call for a five-year ban on the police use of facial recognition and predictive policing algorithms, as part of an international concern over levels of surveillance by states and private actors which the UN considers to be incompatible with fundamental rights (e.g. where individuals have gathered to protest the use of facial recognition can serve to intimidate and deter people from protesting).

Connon et al.'s (2023) analysis of the existing legal frameworks outlines a number of insights and recommendations that need to be considered for the adoption of emerging technologies in policing. As they point out there are a number of **lessons to be learned through the examination of the Information Commissioner's enforcement action, as well as the common law**. The ICO's (2021) investigative report into mobile phone data extraction by police in Scotland is of particular note. Concerns around cyber kiosks included lawful basis for processing and the transparency of information provided to the public and although the ICO acknowledged there had been progress they made a number of recommendations, (e.g. ensuring DPIAs are in place and are reviewed and updated and consulting with the ICO on any proposed high-risk processing of data) see ICO 2021 (cited in Connon et al. 2023: 110). Connon et al. (2023: 111) also mention the ICO's reprimand to the Scottish Government and NHS National Services Scotland in relation to the NHS Scotland Covid Status App.

In relation to both cases Connon et al. (2023) draw out a number of lessons learned including the critical importance of:

1) mapping the relationship between those involved in the development and implementation of emerging technologies (particularly significant when data is being shared between organisations including private to public sector) in order to determine roles and responsibilities in the protection of personal information.
2) understanding the nature of the data being processed and the scope of processing in order to be clear on lawful basis of processing, the need for consent and the information that needs to be provided to the data subject (e.g. there would be an issue if data collected on lawful basis of being necessary for prevention, investigation or detection of criminal offence if it was used to train a commercial algorithm as consent should then be the lawful basis).
3) A comprehensive review of the above considerations must be undertaken *before* deployment of technologies.

Beyond the UK, although the UK is no longer bound by the EU Charter of Fundamental Rights as Connon et al. (2023) argue that in contexts with high potential for a cross boarder dimension compliance with the EU interpretation of Article 8 (Protection of Personal Data) should be taken into account when considering deployment of technologies that are dependent on the processing of personal data. For details of the implications of case law in determining compliance with data protection law and Article 8 in relation to electronic databases, biometric identification systems and surveillance and tracking systems, please see Connon et al. (2023:113-128). In summary, electronic databases should have policies in place that offer clarity on the circumstances in which data will be retained and the purposes for which it is used.

In relation to biometric identification systems the conclusions of the court in relation to the Bridges decision contain important considerations.[18] These include the acknowledgement that the more intrusive the act the more precise and specific the law must be to justify it and public authorities' duty to take steps to make enquires about the potential impact of AFR

[18] Microsoft Word - R (Bridges) -v- CC South Wales ors Judgment.docx (judiciary.uk)

(across protected characteristics) to satisfy equality duty before during and after a trial, and that assessment of impacts should include a mechanism of independent verification. Furthermore, critical issues regarding the interaction between private entities and law enforcement in the development and use of biometric systems were brought into sharp focus by the role of Clearview AI's facial recognition tool, the use of which has been challenged in several jurisdictions (see Connon et al. 2023: 117) e.g. on the basis of failure to obtain consent and process information fairly with lawful reason or meet data protection standards. The critical issue was the lack of lawful basis but in the Canadian investigation for example the potential discriminatory impact of facial recognition technologies was emphasised.[19] The UK ICO investigation also highlighted the issue of commercial advantage and issued and enforcement notice (including a requirement to delete any personal data of subjects residing in the UK from the Clearview Database) and monetary fine of £7,552,800.[20] Daly et al. (2023) highlight that no specific legal framework exists for facial recognition in policing in England and Wales (with existing regulation focusing on fingerprints and DNA evidence) and argue that the Bridges case demonstrates the need for more legal and policy activity to regulate facial recognition.

As Connon et al. (2023) argue policing organisations need to consider how emerging technologies are positioned within regulatory regimes applying to private and public actors. The Council of Europe Guidelines on addressing human rights impacts of algorithmic systems[21] make clear that the impact on human rights must be considered at every stage. They also produced specific guidelines on the use of facial recognition[22] which state that necessity has to be assessed together with the proportionality to the purpose and impact on the rights of the data subjects. Crucially, they highlight that the legal framework should be in place addressing each type of use and providing a detailed explanation of the specific use and purpose; the minimum reliability and accuracy of the algorithm used; the retention duration; the possibility of auditing these criteria; the traceability of the process and safeguards.

Although the SBC code of practice will address the acquisition, retention, use and destruction of biometric data for policing purposes, and data protection law must also be complied with for all processing of personal data, Connon et al. (2023) argue that there is more that can be done to provide a supportive framework for the use of emerging technologies including biometric identification systems. Connon et al. (2023) highlight good practice from New Zealand Police which will be covered in chapter 5 but a couple of implications for legal frameworks are briefly highlighted here. Work by Lynch et al. (2020 and Lynch and Chen (2021) highlighted that the more sensitive the information being

[19] "Face Recognition Vendor Test, Part 3: Demographic Effects," *National Institute of Standards and Technology* (NIST), December 2019 cited in the Joint investigation of Clearview AI, Inc. by the Office of the Privacy Commissioner of Canada, the Commission d'accès à l'information du Québec, the Information and Privacy Commissioner for British Columbia, and the Information Privacy Commissioner of Alberta, PIPEDA Findings 2021-001. February 2021.
[20] ICO Monetary Penalty Notice: Clearview AI Inc Monetary Penalty Notice (ico.org.uk)
[21] Recommendation CM/Rec(2020)1 of the Committee of Ministers to member States on the human rights impacts of algorithmic systems. Appendix
[22] Recommendation CM/Rec(2020)1 of the Committee of Ministers to member States on the human rights impacts of algorithmic systems. Appendix. Para 12.

processed the greater need for specific legal structures to authorise processing and ensure necessary reliability, transparency, and accountability.

In relation to surveillance and tracking devices, Connon et al. (2023) highlight the Canadian Directive requirement that regulated entities undertake an algorithmic impact assessment[23] (using an open source tool) prior to adopting systems dependent on them. Connon et al. (2023) argue that if a compulsory algorithmic impact assessment was being considered it would need to be tailored to the policing context (because algorithms have potential to mask, exacerbate and escalate human biases and there are currently no minimum scientific or ethical standards an AI tool must meet before it can be used in the criminal justice system). In summary, Connon et al. (2023) identified specific legal concerns in relation to automated decision making and the use of AI.

Turning to AI and the European Union, Daly et al. (2023) point out that although 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. The proposed AI Act is a domain-neutral proposal that cuts across sectors and the private-public divide and so it originally was intended to apply to police and other law enforcement actors in the EU. The Act covers development, placement on market and use of AI systems (though there is less of a focus on use). They Act uses a risk-based approach that creates four categories, with a scale of legal constraints. It distinguishes between systems that pose:

a. an unacceptable risk and are therefore generally prohibited (though law enforcement enjoys a number of exceptions);
b. high risk systems that are permitted but more heavily regulated;
c. limited risk systems to which some regulation applies;
d. minimal risks systems that are not regulated, though the development of an adherence to codes of practice and similar frameworks is encouraged.

The use of AI by police potentially cuts across all four categories, though it is explicitly referred to under the rules pertaining to a) and b). Given the broad definition of AI which includes statistical analysis software and some software routinely used by law enforcement agencies for some time without raising particular concerns (or at least not concerns framed in the language of trustworthy AI) could fall under the high-risk category (e.g. automated number plate recognition or forensic DNA matching). It is worth considering some of the implications of the EU's AI Act for a post-Brexit UK and Scotland outlined by Daly et al. (see 2023: 66-67) including: a) direct legal implications (from extraterritorial scope); b) pragmatic implications (de facto regulatory pressure for UK businesses and law enforcement); c) whether the Act provides a good blueprint for Scotland.

a) Legal implications: the Act has some extraterritorial reach in providing safeguards for residents within the EU against use of their data by providers of AI services located abroad (including Scotland). For example, in principle even if data of EU citizens had been transferred lawfully for processing to a third country outside the EU under EU data protection law the processing of the data may fall foul of the additional requirements of the

[23] Algorithmic Impact Assessment Tool - Canada.ca

AI Act creates when the processing involves automated analysis and decision-making using AI. This has implications for UK businesses providing AI services that also involve residents of the EU, and it could potentially affect cross-border police cooperation and data sharing.

b) Pragmatic implications: Daly et al. (2023) argue that the EU's aspirations are that the AI Act will become a global standard and the proposal is already having some international impact (e.g. in Brazil), and the US is also stepping up its efforts to regulate development and use of AI systems.

c) The AI Act as a regulatory blueprint within the UK including Scotland? Daly et al. (2023) note that the Act aims to minimise trade barriers for AI products and services within the EU Single Market which means that it pre-empts the ability of member states to regulate in response to local conditions. 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. The EU Act is domain independent but presumably a Scottish AI Act could only regulate those uses of AI that are devolved matters so a more domain specific approach would be preferable. However, the current UK –wide approach to AI regulation is to issue a set of non-statutory cross-sectoral principles on AI. Daly et al. (2023) argue that 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.

In looking **towards a fair future** Daly et al. (2023) conclude that whilst Police Scotland are now more mindful of the ways in which Article 6 ECHR (right to a fair trial) is engaged in carrying out their functions there has been limited analysis of how policing activities with digital technologies may engage ECHR Article 8 (right to private life) or have specific impacts for the protected groups in EA 2010. In addition they point out that there are distinct and emerging risks that widespread use of surveillance tools and AI-enabled technologies may undermine citizens' digital right and hider their willingness to meaningfully participate in democratic processes.

Therefore, Daly et al. (2023) argue that Scottish Minsters, 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 emerging technologies in policing. This includes incorporating equality and human rights legal frameworks and principles into new legislation, codes of practice and guidance. For example, a position that the issue of legal basis for cyber kiosks should be settled by litigation is not consistent with a best practice philosophy, transparency or accountability.

A number of recent engagements in Scotland on emerging technologies and policing are mentioned by Daly et al. (2023) with the assertion being that a human rights based should be more front and centre e.g. in the in the SPA working group on options for the future delivery, accreditation, oversight and governance of digital forensics in Scotland. The Biometrics IAG did provide a human rights analysis (incorporating the PANEL principles) and develop a draft Code of Practice.

Chapter 4 summary and conclusion

Further to policing legislation, key domestic and international legislation and relevant case law relating to emerging technologies in policing including Human Rights, Equalities, Data Protection, Biometrics and Law of Evidence was reviewed. Impacts on rights and freedoms include privacy, discrimination etc. and may also occur at a societal level, but interference with democratic freedoms should only be permitted if it is lawful, proportionate and necessary. On the other hand, with regulation and governance of design and development, emerging technologies such as AI may be used to advance, rather than put at risk, equality and human rights (e.g. real time translation could support right to a fair trial).

However, specific concerns exist in relation to automated decision making and the use of AI in policing surrounding data protection, transparency and potential to exacerbate bias and discrimination. Although guidelines and an accountability framework for AI exist at UK level these are not legally binding. Live Facial Recognition raises human rights (proportionality concerns) as well as being potentially discriminatory. Indeed, The Ryder Review recommended a legally binding code of practice for live facial recognition should be formulated.

In conclusion, Daly et al. (2023) argue that there would be an advantage to Police Scotland in considering that Article 8 is engaged wherever their technology is used to collect data (including general or targeted surveillance) that could on its own, or in conjunction with other data, identify people or personal characteristics. Police Scotland need to ensure and enhance its approach to data protection compliance to ensure data protection by design and default and to ensure all risks to the rights and freedoms of individuals are identified, assessed and mitigated in DPIAs. In addition, Daly et al. (2023) argue that in line with Scotland's National Action Plan for Human Rights, Police Scotland should further embed a human-rights based approach within the structures and culture of policing, including strengthening human rights training and accountability e.g. evaluating the use of emerging technology or change of use of existing technology by using the PANEL tool. 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. As part of demonstrating due regard to the needs of the PSED, equality should also be embedded in these areas. Daly et al. (2023) argue that by embedding human rights-based decision-making Police Scotland will have less need to engage in corrective action in response to external pressure. Their approach could be enhanced by internalising human rights knowledge and capacity e.g. by employing equality and human rights experts to assist in policy design, delivering training and supporting officers in order to mainstream knowledge.

A number of key considerations relating to legal frameworks for emerging technologies in policing in Scotland are outlined here but may be found in full in Appendix C.

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

4.2 The **impacts** of new technologies in policing **on human rights and equalities need to be further considered** e.g. via the 6th ethics and human rights case (see ch8) and risks must continue to be assessed and mitigated throughout the lifecycle.

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

4.4 Whilst significant legislative gaps were not found, Scottish Government (and where appropriate the SBC) should seek to **keep the legislative landscape under review** and consider whether future technological deployments (such as Live Facial Recognition and certain applications of AI, e.g. in predictive policing) would benefit from the **introduction of statutory codes of practice in order to provide greater clarity and safeguards**. The possibility that certain applications of some technologies in policing should be **categorically prohibited from use**, either because they are **unacceptably risky** even with mitigation in place, or because they are intrinsically incompatible with human rights, should be considered in this context by Government.

4.5 Policing bodies must have **special regard to the interests of children and vulnerable persons** and how the technologies may impact upon them.

4.6 The use of new technologies should **not unlawfully or unjustly adversely impact an individual or group of individuals** and the processing should be within the reasonable expectations of the public.

4.7 Police Scotland should **seek to publish Operational Practice Codes as soon as possible prior to implementation** of technologies, and **proactive communications** on use and effectiveness post-implementation. The **necessity of drone deployment** rather than other means of investigation must be considered given the likelihood they will capture sensitive personal data and have a high risk of collateral intrusion.

4.8 Attention must be paid to personal data generated by technologies used by policing bodies, **ensuring mission creep is managed and data is processed for specific, explicit and legitimate purposes**. New systems must be in compliance with data protection law and **additional safeguards should apply where processing relates to children and vulnerable people.**

4.9 **Data flows must be mapped and understood so the roles and obligations of multiple partners** (including private vendors) **under data protection law are understood prior to implementation** of data sharing technologies.

5. Ethical and social implications and good practice

This chapter covers ethical considerations including the use of ethics panels and lessons learned in Scotland, social and ethical implications, and good practices in ethical frameworks from other fields and jurisdictions. It is based on the work of the commissioned research report (Connon et al., 2023) and the report of the first workstream of the IAG (Daly et al., 2023), with some input from the oversight, scrutiny and review workstream of the IAG (Ross et al., 2023).

Ethics:

The workstream 4 report (Ross et al., 2023) considers ethics as a system of moral principles that shape how people make decisions, lead their lives and carry out their work. They point out that Police Scotland's Code of Ethics sets out the standards expected of officers and staff, which reflect the values (integrity, fairness, respect and human rights) of the service. As Daly et al. (2023) state, ethical considerations associated with emerging technology in policing can be operationalised through 'live' impact assessment documents (which can adapt to new knowledge), through advisory engagement or debate on proposed initiatives through consultation and panes/forums. Force policies, guidance and training are also important to inform officers and staff about ethical consideration and, standards and the ways in which behaviour is compliant with bias mitigating efforts. As Raab (2020) points out there has been a large volume of work seeking to define principles and frameworks for the ethical use of advanced technologies and there has been a regulatory 'turn' to ethics, including through the use of ethics panels.

IAG public consultation:

As outlined by Daly et al. (2023) some of the responses to the IAG's 'Call for Evidence' discussed ethical dimensions, with both an 'ethical and legal assessment framework' and 'ethics panels' proposed to address challenges relating to ethical standards. Many responses highlighted that introducing technology into operational domains without proper ethical frameworks to engage critical assessment or external consultation is likely to result in negative outcomes for all stakeholders, including eroding public trust. Ethics panels were said to allow subject matter experts from a range of disciplines to independently grapple with the ethical and legal issues associated with emergent policing technologies. It was recommended that practitioner, professional, community and academic voices should be included in such fora. One response suggested that ethics panels should include people who understand power asymmetries in the use of technologies. As ethics panels influence decision making and inform public policy, it was assumed that these spaces should not include individuals or groups with financial interests. It was suggested that ethics panels should embrace an equality and human rights-based approach to understand impacts on individuals and outcomes should provide strong and unbiased evidence on whether the proposed technology will entrench existing inequalities. Clearly this links to considerations from chapter 4.

Ethics advisory panels:

As outlined by Ross et al. (2023), Police Scotland have introduced four tiers of Ethics Advisory Panels (EAPs), which provide an opportunity for staff, officers, and external participants to discuss ethical dilemmas. The ethics panels are not decision-making bodies but provide advice and support to the decision maker (or dilemma holder), who remains responsible for taking the decisions, with due consideration of the panel's views in their rationale. The objectives of panels include improving service delivery, supporting police officers, staff and leaders, developing and enhancing a visible ethics culture and supporting organisational learning.

Information about the four tiers of panels may be found in Ross et al. (2023: 20-21) and Daly et al. (2023: 39-41) but in short, Regional Panels (North, East and West) focus on ethical dilemmas that impact on local and or operational decision making and are comprised of staff and officers and chaired by trained senior officers and staff. National Panels will focus on ethical dilemmas which impact upon national, strategic and tactical decision making and comprise those with a national remit and chaired by trained senior officers and staff. The Independent Panel is chaired by an independent member, with DCC Professionalism in co-chair, and considers dilemmas that impact public service and confidence (e.g. Remote Piloted Aircraft Systems, BWV), providing external consideration and scrutiny from members drawn from a broad spectrum of society, to advise the decision maker. Chaired by the Convenor of the Scottish Youth Parliament's (SYP) Justice Committee (with CIU Ethics and Preventions holding the role of PS Delegate), the Youth Panel sits parallel to the Independent panel and is run in partnership with the SYP with trained MSYP's engaging the voice of Scotland's young people in police decision making.

It should be noted that the Regional and National EAPs only have internal Police Officers or Staff in attendance and the organisation would benefit from ensuring that externals are present at these to ensure a variety of subject matter expertise. Whilst EAPs may help Police Scotland to improve service delivery and consider ethical implications when deliberating the implementation of new technologies there is not currently a clear expectation of inclusion of the findings in the Full Business Case template. Therefore, a clear explanation of how the findings and advice from the EAPs helped shape the solution, planned implementation or preferred option for the new technology should be included in a new section of the FBC template. This links to a recommendation from chapter 8 (key consideration 4 in Ross et al. (2023) to develop a sixth ethics and human rights case in Business Cases.

In my view as Chair, in addition to improving clarity on action taken as a result of EAPs i.e. how the findings/advice from ethics panels are used to shape decision making there and embedding these expectations in oversight e.g. through business cases there are potentially some further enhancements that could be made to ethics panels. For example, it does not appear that minutes are made public so it is suggested that anonymised minutes or a summary of meeting discussions and outcomes are published (either publicly by Police Scotland or to relevant SPA committees) order to enhance transparency.

Reflections from Dr Marion Oswald (Daly et al. 2023: 40) on Police Scotland's Ethics Advisory Panels suggest that it is important to link the administrative or committee arrangements that are being established to operationalise the framework in order that there are clear oversight processes to ensure the framework is implemented (and it is not just

principles on paper). Oswald points out that the proposed structure is quite different to the structure of structure of West Midlands PEC and Police Data ethics Committee (West Midlands police website) 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. Although Oswald acknowledges there are still many issues (Marion Oswald research paper) with this sort of oversight, including the relationship with legal compliance and practical issues around budget and resourcing, the 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. Oswald questions whether Police Scotland's EAPs have the expertise and independence to influence technological developments within the force. She also emphasises that consideration should be given to how EAPs could be involved in a system of rolling review, from proposal/pilot to implementation in order to track progress and give ongoing advice.

Data ethics framework:

Data and data-driven technology provides new opportunities and the potential for innovation but this needs to involve responsible and trustworthy use of data. Police Scotland's new Data Ethics Framework will guide this responsible use and provide governance required to identify and address ethical challenges posed by novel uses of data and data-driven technology. It has been developed in collaboration with the Centre for Data Ethics and Innovation (CDEI) and through engagement across policing and externally. It is being introduced in order to ensure that 'data-driven' technology solutions are using data responsibly, and any associated data ethics risks are identified, managed, scrutinised (internally and externally) appropriately. Whilst the Independent Ethics advisory Panels address the 'should we' type of individual ethical dilemmas, the Independent Data Ethics Group (similar to WMP) will focus on the 'how do we' implement the new data-driven technologies, typically reviewing project proposals. For more information on the Data Ethics Framework see Police Scotland's account (Daly et al. 2023: 42) and for its role in governance see Chapter 8 below and Ross et al. (2023).

The framework is principles based, using questions which encourage robust, evidence-based responses and are open to internal and external scrutiny in order to enhance trustworthiness. Key themes covered in the questions include: value and impact (measured and evidenced benefit to individuals or society); effectiveness and accuracy (assess ability to improve accuracy, with a need for monitoring or independent evaluation for sensitive projects); necessity and proportionality (intrusion must be necessary to achieve policing aims and be proportionate in relation to benefits); transparency and explainability (ensuring purpose, details and notice of deployment are understandable and made public and open to scrutiny); reliability and security (measures in place to ensure data is used securely and protects privacy). This approach is designed to help the policing system in Scotland to use data ethically by helping to identify potential harms, risks and challenges and weigh these up with potential benefits and opportunities.

The approach of the framework to embedding good governance (see chapter 8) is anticipated to contribute to building public confidence but also to assist with: *being transparent and open* (communicating uses clearly ad accessibly and proactively where possible); *engaging with diverse views* (and where possible demonstrating the path to impact such engagement has); *drawing on specialist and multi-disciplinary expertise* (to

ensure the use of data and data-driven technology is robust, evidence-base and effective); *clearly articulating the purpose and value* (and ensuring these are measured and met and include trade-offs and public acceptability); *identifying and mitigating potential harms*; *creating an environment for responsible innovation* (where new approaches are explored within frameworks of rigorous oversight, evaluation and transparency).

Reflections from Dr Marion Oswald (Daly et al. 2023: 43) on Police Scotland's Data Ethics Governance Framework acknowledge the value the adoption of a triage process to identify high risk applications. Oswald highlights the value of long-term and robust evaluation methods and the importance data and outputs of data-driven technology being accurate and not leading to detrimental unintended consequences. Oswald emphasises how crucial it is to publish papers, advice and minutes relating to the new Independent Data Ethics Scrutiny Group and the need to allocate budget for secretariat support.

In summary, Daly et al. (2023) conclude that ethical considerations around emergent technologies in policing 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 include technology enabled mass surveillance or social sorting, expansion of use cases of technology (i.e. function creep), potential chilling effect on populations, collateral intrusions, and insufficient safeguards surrounding analytical capabilities. Independent oversight of ethics processes and due transparency over them is crucial to ensuring ethical outcomes.

Lessons learned and good practices relating to ethical considerations:

Some of the lessons learned and good practices highlighted by Daly et al. (2023) through the Scottish case studies are of relevance here. In relation to Cyber Kiosks, when it comes to viewing the contents of an individual's mobile device there are many ethical contentions that arise. For example, potential for collateral intrusion to occur (intrusion into private life of friends, family, and other people situated in the social network of the individual). In addition, there is potential for police overreach (if not target searches of personal data may be viewed and invasive levels of privacy interference may occur).

The End of Project Report (ERP) for Cyber Kiosks recognised there was not full consideration of or consultation with relevant stakeholders' concerns relating to the use of Cyber Kiosks and there was not enough time spent considering public perceptions or concerns. Therefore, public consent, public concern, engagement and consultation and ethical considerations should be addressed in future through effective risk management, via business cases (following HM Treasury Green Book's framework and accounting for ethical considerations) and impact assessments. Police Scotland asserts (Daly et al. 2023: 52) that lessons learned through Cyber Kiosks have resulted in improvements relating to the implementation of policing technologies e.g. through the involvement of external stakeholders and reference groups and the use of post implementation reviews and enhanced governance (business cases, EqHRIA, DPIA etc.).

Social and ethical implications:

This section summarises findings from a review of literature undertaken by Connon et al. (2023: 27-59) for the IAG to explore various social and ethical implications associated with three broad categories of technology type: electronic databases, biometric identification

systems; electronic surveillance and tracking devices. This is based on a systematic review of interdisciplinary social sciences research literature on the development, trial and implementation of emerging technologies in policing.

Electronic databases:

Connon et al. (2023: 27-28) describe what is meant by electronic databases and consider various specific types of electronic database technologies and uses discussed in the literature. **Data sharing and third-party data sharing platforms** raise a number of social and ethical issues under the following themes: safety of information held; human rights and privacy; lack of standardisation and accountability; differences in organisational practice; bias embedded in data, data organisation and data sharing processes. Ensuring the safety of information held and preventing data breaches is central in for example: preventing risk of increased victimisation, inequalities or inefficiency (Clavell, 2018); building public confidence and facilitating information sharing with the police online as well as in person (Aston et al., 2021a).

In relation to human rights and privacy, for example, Holley et al. (2020) highlights concerns with decentralisation and fragmentation of security of personal information, with greater control to private security governance professionals. Neyroud and Dilsey (2008) argue that the effectiveness of electronic databases in detecting and preventing crime should not be separated from perceptions of legitimacy and ethical and social questions surrounding the impact on civil liberties. Therefore, as they argue strong transparent management and oversight of these technologies is essential, including ensuring integrity and reliability of the technology, alignment between purpose and use in deployment, transparency in governance, and ensuring public confidence in the technology. McKendrick (2019) argues for broader access to less intrusive aspects of public data and direct regulation (including technical and regulatory safeguards to improve performance and compliance with human rights legislation) of how those data are used – including oversight of activities of private-sector actors. It is worth noting that private sector actors should only be processing personal data collected for policing purposes when acting as a processor for a competent authority or if data is shared with them by a competent authority (who has obligations to ensure this complies with DP law). As data flows are complex DP must be considered at the design and procurement stage.

In relation to lack of standardisation and accountability Babuta and Oswald (2020) note that there is a lack of organisational guidelines or clear processes for scrutiny regulation and enforcement and these standards and clear responsibilities for policing bodies in relation to them should be addressed as part of a new draft code of practice. Differences in organisational practices can result in digital divides and problems with data integration (Sanders and Henderson, 2013). Bias embedded in data, data organisations and data sharing processes can include data containing existing biases reflecting over-policing of certain communities (e.g. disadvantaged socio-demographic backgrounds) and racial bias which are reproduced by the application of datasets (Babuta, 2017).

Community policing applications raise risks of enhancing racial inequalities e.g. via community–instigated policing such as the Nextdoor app which embeds unchallenged racist attitudes in neighbourhood monitory data (Bloch, 2021) and exacerbation of inequalities via use of community policing apps as part of hot spots policing (Hendrix et al., 2019). Instead of enhancing inclusion and social and technological capital, community policing applications

can widen the gulf in participation and community-police relations and result in inequalities between those who provide information and those whose information is being recorded (Brewster et al., 2018). Maintaining public trust is a central issue, for example van Eijk (2018) argue that transparency about the aims of engagement and how data will be held, O'Connor (2017) stresses that visibility and storage of information must be considered and Aston et al. (2021a) emphasise key concerns around anonymity and privacy of information, risk of abuse of personal data and the importance of allowing people to opt out of having personal data stored.

Challenges in relation to **data pulling platforms** include inequalities in police resources impacting the utilisation of big data and its integration with administrative and open data sources and platforms impacting effectiveness (Ellison et al. 2021) and different culture and practices in various sectors regarding collection, sharing, processing and use of different types of data creating shifts in distribution of power between various sectors (National Analytics Solutions 2017).

Social media platforms and data storage raises a number of issues including lack of alignment in organisational culture impacting the collection, storage, management and use of social media data. This means, for example, that social media has not helped facilitate the desired interaction between police and communities in England (Bullock, 2018) and the lack of clear policies and guidance for the collection, management and use of social media data pose a potential ethical risk (Meijer and Thaens, 2013). With regard to the legitimacy of police action the availability of social media data can be used by the public to question police over their practices (Ellis, 2019), whilst Goldsmith (2015) highlights reputational problems for off-duty use of social media by police officers. Issues with the management of use of sensitive information obtained through social media data are raised in relation to use in police surveillance activities, digital forensics and covert online child sexual exploitation investigations and the ethical issues with extended surveillance and storage of data (Fussey and Sandhu, 2020). Risks of enhancing actual and perceived social injustices posed by social media include unprecedented capacities to monitor the police and expose injustice (Walsh and O'Connor, 2019), but also the ability to monitor social media data streams risk enhanced surveillance of particular community groups which may negatively affect police-community relations (Williams et al., 2013).

Open-source data can result in increased victimisation if not adequately managed (Clavell et al., 2018), may 'drive' predictive policing strategies and sometimes unnecessary pre-emptive police action (Egbert and Krausmann, 2020) and can lead to over-policing in the sphere (Kjellgren, 2022).

Vulnerable population databases and datasets raised various issues including surveillance of vulnerable populations for example, improperly restricted data availability and lead to disproportionate profiling, policing and criminalisation of marginalised groups (Hendl et al., 2020) and the importance of guidance as to how and when information should be shred (Storm 2017). Issues of human rights and justice include the potential for discrimination through systematic marginalisation and Malgieri and Niklas (2020) highlight issues of consent and call for vulnerability aware interpretation. They also called for greater communication with vulnerable people as to how data is stored and used and Lumsden and Black (2020) discuss the importance of ensuring data and service areas responsive to needs of deaf citizens. Lack of guidance and prioritisation for data collection and

management is an issue e.g. Babuta (2017) calls for the development of a clear decision-making framework to ensure ethical use of vulnerable population data.

Biometric identification systems:

Facial recognition technology literature raised various social and ethical issues including trust and legitimacy, identified by Bradford et al. (2020) as important factors in the acceptance and rejection of these technologies, whilst McGuire (2021) explains that perceptions of misuse of technologies and denial of rights can threaten the viability of policing. As Bragias et al. (2021) argue, a deterioration of police-citizen relations, with the public often being sceptical about how the police will use the technology and for what purposes. It also carriers a risk of enhancing inequalities for marginalised groups, with police concerns including anti-discrimination law (Urquhart and Miranda, 2021) and Hood (2020) discussing the dangers of integration of facial recognition into police body-worn camera devices and risks of reinforcing racial marginalisation. Furthermore, Chowdhury (2020) argues that even with improved accuracy facial recognition technologies, used disproportionately against people and communities of colour, will likely still exacerbate racial inequalities. Privacy and security concerns raised include the right to respect for private life (Keenan, 2021). Lack of standardised ethical principles and guidance were raised by Babuta and Oswald (2017).

Artificial intelligence raised issues including reproduction of systemic bias of human decision makers in predictive policing (Alikhademi et al., 2022). Issues of accuracy fairness and transparency include bias and lack of operational transparency (Beck, 2021), with decisions of algorithms viewed as less fair than a police officer decision (Hobson et al. 2021), with Asaro (2019) raising concerns about treating people as guilty of future crimes for acts they have not committed or may never commit. Risks of racial and gender bias may be embedded in the design and implementation (Noriega, 2020) of AI technologies, although the potential of AI to promote a non-biased environment was also acknowledged. There was a call for clear ethical guidelines and laws to minimise potential harms associated with AI in policing. The risk of potential use of AI by perpetrators of crime was acknowledged (Hayward and Maas, 2021).

Voice recognition technologies and mobile, cloud, robotics and connected sensors are associated with concerns related to: privacy and security and political and regulatory factors affecting interoperability and concerns about standards (Lindeman et al., 2020), human rights and a lack of well-established norms covering the use of AI technology in practice (McKendrick, 2019).

Surveillance systems and tracking devices:

Drones raised issues relating to legitimacy of use of unmanned devices by police departments (Miliakeala et al., 2018); issues of the development of an arial geopolitics of security e.g. implications for power relations (Klauser, 2021); public confidence and trust e.g. issues with using drones to monitor political protest in the US (Milner et al., 2021); concerns relating to racial biases in deployment, with e.g. Page and Jones (2021) questioning the ability of drones to make policing more efficient and ‘race-neutral’; and

serious concerns about use in domestic policing personal privacy and intrusion of surveillance in people's daily lives (Sakiyama et al., 2017).

Smart devices and sensors raised key ethical issues relating to privacy e.g. concerns regarding the level of increased surveillance (including to officers) posed by highly networked systems (Joh, 2019); trust and legitimacy of police use e.g. Joyce et al. (2013) emphasising it requires ongoing collaboration with the public and researchers.

Location and 'Hot' Spot' analysis tools literature discuss issue relating to effectiveness in reducing crime with the applications being used for surveillance and enforcement and having little if any direct measurable impact on officers' ability to reduce crime in the field (Koper et al., 2015). The use of advanced electronic monitoring schemes (combining GPS tracking and radio frequency technology) in the context of privatisation of probation in England and Wales raises challenges concerning the legitimacy of product selection given enquiries relating to providers overcharging the government for their services (Nellis, 2014). Lack of guidance or integration of technology within specific crime reduction agendas raises concerns about policing adopting technologies without giving consideration to how they fit within their operational goals (Hendrix et al., 2019).

Body worn video cameras literature highlighted implications for public-state relationships e.g. Hamilton-Smith et al. (2021) found that technologies such as hand-held cameras and BWV had a detrimental impact on police-fan relationships, interactions and dialogue. In relation to impacts on police officers and police practice Henne et al. (2021) argue that the use of BWV redefines police violence into a narrow conceptualisation rooted in encounters between citizens and police and direct attention away from the structural conditions that perpetuate violence. Miranda (2022) concludes that use of cameras and how they operate technically, raise ethical issues for data management and storage. Concerns about racial biases inherent in deployment of the technology were raised by Hood (2020) regarding racial marginalisation, and Murphy and Estcourt (2020) who argued they could contribute to over-surveillance of minority communities.

Serious ethical challenges with **autonomous security robots** were discussed by Asaro (2019) as they can potentially deploy violent and lethal force against humans and there is increased interest in developing and deploying robots for enforcement tasks, including robots armed with weapons. Though not usually acceptable, police officers are authorised by the state to use violent and lethal force in certain circumstances in order to keep the peace and protect individuals and the community from an immediate threat and therefore the design of human-robot interactions (HRIs) in which violent and lethal force might be among the actions taken by the robot pose problems.

CCTV and visual/optical technologies pose concerns regarding a lack of standards and principles (Brookman and Jones, 2022), with Clavell et al. (2018) arguing that if they are not managed correctly, they can result in increased victimisation, inequalities or inefficiency.

Best practices:

Connon et al. (2023) also outline best practice for implementation and dissemination from research and policy relevant literature on electronic databases, biometric identification systems; electronic surveillance and tracking devices

Electronic databases:

Recommendations for improving **databases and third-party data sharing** include better *management of expectations and communication of the needs* of different organisations to strengthen interoperability of working with multiple datasets as well as manging data subjects' privacy and human rights (Neiva et al., 2022), and the need for greater *material, social and organisational integration* to enable effective use of technologies (Sanders and Henerson, 2013). Neyroud and Disley (2008) argue that strong *transparent management and oversight* of data sharing technologies with third party organisations are essential. McKendrick (2019) recommend *clear transparency* regarding the handling of data, especially by private companies and *clear information and communication* as to data access and limitations by third parties.

The National Analytics Solutions (2017) provide specific guidance for greater *standardisation of practices* and argue there is a need for greater clarity over legal obligations on data storage and processing across all parties, consent issues relating to data subjects and the duration of storage (see Connon et al., 2023: 83). They provide an ethical framework (underpinned by four dimensions of society, fairness, responsibility and practicality) for data management and sharing. Babuta (2017) recommends *standardisation of concepts* for entering information into police databases and the creation of Multi-Agency Safeguarding Hubs (MASH) for better data sharing practices underpinned by the development of a *clear decision-making framework at the national level to ensure ethical storage, management and use of data*.

Regarding **social media platforms and data** Williams et al. (2021) recommends greater cooperation between policymakers, social science and technology researchers for the development of *workable, innovative guidance for working with social media data* in the policing of hate crime and malicious social media communications. In relation to **vulnerable population databases and datasets** Asaro (2019 recommends an Ethics of Care approach to the management of use of data whereas Babuta (2017) suggest that MASH databases would help facilitate this. **Community policing applications** literature argues that improvements to *data storage systems and protections and procedures* may help improve public confidence in policing and information sharing (Aston et al. (2021a) and Clavell et al. (2018) present a set of *ethical guidelines*.

Biometric identification systems:

Recommendations pertaining to the use of **facial recognition technologies** focus on improving public support and emphasise the need to devise new ethical principles and guidelines for its use including calling for: *transparency* (Bragias et al., 2021); *interrogation*

of biases prior to development (Williams, 2020); a *draft code of practice* (Babuta and Oswald, 2020); *clear ethical principles and guidance* implemented in a standardised manner (Smith and Miller, 2022); further *trials* (National Physical Laboratory and Metropolitan Police Force, 2020)[24]; and a *generational ban until further guidelines* (plus mandatory equality impact assessments, collection and reporting of technicity data, independent audits etc.) and legal stipulations have been developed (Chowdhury, 2020).

In relation to **Artificial Intelligence** the focus of the existing research is on minimising biases towards marginalised communities, establishing standards for predictive policing technologies and raising awareness. Asaro (2019) recommends an *AI Ethics of Care approach*, taking a holistic view of values and goals of system designs, whereas Whittlestone (2019) argues that *high level principles* can help ensure costs and benefits of use of technologies for marginalised groups should be weight up prior to implementation for specific purposes. Alikhademi et al. (2022) develops a s*et of recommendations for fair predictive policing to minimise racial bias* including pre-processing of data to reduce dependence on variables identified as discriminatory, use of counterfactual analysis processes to detect and correct bias, post-processing of results to make the respect group and individual fairness and analysing results to evaluate the fairness of outcomes for groups (see Connon et al., 2023: 90).

Surveillance technologies and tracking devices:

In relation to **location and 'hot spot' analysis technologies** Koper et al. (2019) call for *greater training on strategic uses* of IT for problem-solving and crime prevention and greater attention to behaviour effects of technology on officers and Hendrix et al. (2019) suggest that police should *improve planning regarding how these forms of technology fit within operational goals* and guiding philosophy. Regarding **body worn video cameras** Lum et al. (2019) emphasise that to maximise positive impacts more attention needs to be paid to the ways and contexts (organisational and community) in which BWV are most beneficial or harmful and address how they can be used in police training, management and internal investigations to achieve long-term potential to improve police accountability and legitimacy. Murphy and Estcourt (2020) recommend that the public should be involved in the formulation of police guidelines concerning the use of BWV whilst Todak et al. (2018) recommend a comprehensive planning process that incorporates the views of all stakeholders in implementation.

Asaro (2019) states that given serious challenges of automating violence at the very least the use of **autonomous security robots** requires the development of strict ethical codes and laws, but ultimately argues that their *use should be banned* in policing. Pertaining to **CCTV and visual/optic technologies** recommend the need to introduce and refine clear standards and principles concerning their use in forensic investigations (Brookman and Jones, 2020).

[24] met-evaluation-report.pdf

Best practice in ethical frameworks:

Drawing on research for the development of ethical standards in relation to **facial recognition technologies** Almeida et al. (2021) argue for the need for better checks and balances, transparency, regulation, audit etc. and pose *ten ethical questions* to be considered for ethical development, procurement, rollout and use. These include who controls the development, purchase and testing to challenge bias; the purposes and contexts for use; what specific consents, notices and checks and balances should be in place for these purposes; the basis for building facial data banks and consents, notices checks and balances in place for fairness and transparency; limitations of performance capabilities; accountability for different usages and how it can be audited; complaint and challenge processes; and counter-AI initiatives to test and audit (see Connon et al., 2023: 96).

On **Artificial Intelligence,** Whittelstone et al. (2019) explore various *published prescriptive principles and codes* e.g. Asilomar AI Principles that list ethical and values AI must respect, Partnership on AI which established a set of criteria guiding the development of AI which technology companies should upload, five principles form the House of Lords Select Committee on AI and the cross-sector AI code, Global Initiative on Ethics of Autonomous and Intelligence Systems' set of principles for guiding ethical governance and found substantial agreement and overlap between different sets of principles. Oswald (2019) draws on lessons learnt from the West Midlands data ethics model to recommend a three-pillar approach (law plus guidance and policy interpreted for the relevant context; ethical standards attached to personal responsibility and scientific standards and a commitment to accountability at all levels) to achieving trustworthy and accountable use of AI and the lessons that can be learned including in relation to effective accountability and the role and necessity of human rights framework in guiding the committee's ethical discussion. Oswald recommends that a national ethics approach would require clear scientific standards that are written with the policing context in mind.

Dechesne (2019) draws on research and lessons learned from policing in the Netherlands to develop a *set of recommendations for the responsible use of AI to ensure alignment with ethical principles*. These include: creating an AI review board and considering an AI ombudsperson to ensure independent critical evaluation; updating the organisational 'code of ethics'; incentivising the inclusion of ethical, legal and social considerations in AI research projects; training AI scientists on ethical consideration; developing a regress process; clear processes for accountability and responsibility; evaluation procedures; auditing mechanisms; measures to prevent, detect and mitigate errors; transparent systems to enable accountability; respect for privacy; and human agency (see Connon et al. 2023: 98).

Lessons learned from health, children and family sectors:

Connon et al. (2023: 102-107) also cover lessons learned from research on the trial and adoption of emerging technologies in the health, children and family sectors. With regards to **electronic databases** Faca et al. (2020) examined *ethical issues with digital data and its*

use in relation to minors within the health sector, including consent, data handing, minors' data rights, private versus public conceptualizations of data generated through social media and gatekeeping. Concerns were raised regarding the preclusion of minors from important research (given ethical considerations) and the need for greater discussion to co-produce guidelines or standards concerning ethical practice between researchers and minors. Schwarz et al. (2021) explored the effects of sharing electronic health records with people affected by mental health conditions and found access to information about themselves was associated with empowerment and trust (though negative experiences resulted from inaccurate notes, disrespectful language or undiscussed diagnoses) and recommended guidelines and training. This raises important considerations for policing in relation to *setting standards regarding subject access to records held* about them. Birchley et al. (2017) on ethical issues involved in smart-home health technologies emphasise provision of *clear information about the sharing of data with third parties.* It is worth noting that the ICO has produced an Age Appropriate Design Code which certain online services must conform to and is also a useful reference on how to ensure the best interests of the child are considered in any service.

Regarding **Artificial Intelligence** Ronquillo et al. (2021) identified challenges in the context of nursing emphasising the importance of consideration of: professionals need to understand the relationship between the data they collect and the AI technologies they use; the *need to meaningfully involve professionals in all stages* of AI (from development to implementation); the need to address limitations in knowledge so professionals can contribute to the development of AI technologies. Work on **smart devices and sensors** include privacy (Birchley et al., 2017) and privacy and security (Zhu et la., 2021) again arguing professionals should be involved in the design and implementation of these technologies to help promote ethical awareness and practice.

In respect of **lessons learned relating to ethical frameworks** from these sectors in relation to AI, voluntary guidelines on ethical practices (from governments and other professional organisations) are regarded as weak in terms of standards for accountability, enforceability, and participation and for their potential to address inequalities and discrimination (Fukada-Parr and Gibbons, 2021). It is argued that there is a need for *governments to develop more rigorous standards grounded in international human rights frameworks* that are capable of holding Big Tech to account and they recommend that AI guidelines should be honest about their *potential to widen socio-economic inequality* and not just discrimination and that governance of AI design, development and deployment should be based on a robust human rights framework to protect the public interest from threats of harmful application. Leslie (2019) outlines critical components of an ethically permissible AI project (see Connon et al., 2023: 107) including the project being fair and non-discriminatory, worthy of public trust and justifiable. Furthermore, the ICO guidance on AI and data protection provides practical guidance on how to ensure that the use of AI is fair and transparent and how bias and discrimination can be addressed.

Chapter 5 summary and conclusion

Ethical considerations can be particularly contentious and difficult to operationalise in the domain of policing. These can be considered in 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. Police Scotland uses Ethics Advisory Panels and is introducing a new Data Ethics Framework. Force policies, guidance, and training may be used 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. It is important to ensure appropriate safeguards are in place, but there also a need to facilitate adoption of technology in order for police to fulfil their statutory duties. Therefore, the expectations in terms of evidence gathering, evaluation and oversight related to the introduction of new technologies should vary depending on the existing evidence base and level of risk. Police Scotland has many governance processes in place and being introduced to address the ethical issues and independent oversight and transparency over them is central to ensuring ethical outcomes.

Social and ethical issues associated with various forms of emerging technologies explored by Connon et al. (2023) included storage of sensitive information, risks to enhancing social injustices and surveillance of vulnerable groups relating to certain uses of electronic databases. Issues of accuracy, fairness and transparency were particularly discussed in relation to Artificial Intelligence applications and usage in predictive policing. Live facial recognition raised questions regarding trust and legitimacy, privacy, personal security, enhancing inequalities and the lack of standards, ethical principles and guidance were highlighted key gaps. Concerns relating to privacy, surveillance of minorities and public confidence were particularly pertinent when discussing surveillance systems and tracking devices including drones, smart devices and sensors, location and 'hot spot' analysis, body worn cameras, autonomous security robots, CCTV and visual/optical technologies.

Best practice for implementation of emerging technologies in policing highlighted by Connon et al. (2023) include, in relation to electronic databases and third-party data sharing, strong transparent management and oversight; a clear decision-making framework and standardisation of practices regarding data storage, management, sharing and use; better management of expectations and communication of the needs of different organizations to strengthen interoperability of working with multiple datasets as well as managing data subjects' privacy and human rights. Research relating to use of live facial recognition (LFR) technologies focuses on ethical principles and guidelines including calling for a code of practice, transparency, interrogation of biases prior to development, further trials, and a ban until further guidelines and legal stipulations have been developed. In relation to Artificial Intelligence the focus is on various recommendations to minimise biases towards marginalised communities and establishing standards for predictive policing

technologies. Asaro (2019) states that the use of autonomous security robots requires the development of strict ethical codes and laws, but their use should be banned in policing. Best practice in ethical frameworks include for example, ten ethical standards in relation to facial recognition technologies (Almeida et al. 2021), on AI various published prescriptive principles and codes (Whittlestone et al. 2019), and Oswald's three-pillar approach.

A number of key considerations relating to ethical and social implications are outlined here but see Appendix C (and Connon et al., 2023: 4-7) for more details.

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

5.2 Police Scotland and the SPA should **continually improve the use of Ethics Advisory Panels (EAPs) to enhance external involvement and independence, transparency and the role of EAPs in continual review.**

5.3 Consideration could be taken of a number of **potential policy and practice suggestions** highlighted by Connon et al. (2023: 134-139), relating to various technologies (electronic database technologies, biometric identification systems and AI technologies, surveillance systems and tracking devices) which will be of interest and may be found in full on pages 134-139 of the Stirling report.

5.4 a) Policing bodies and scrutiny bodies should **ensure a monitoring mechanism, to record data on its equality and human rights impacts, is incorporated into the design and implementation of an emerging technology**. Police Scotland should routinely gather and use equality information relevant to all protected characteristics, including ethnicity data, which should be reported transparently in order to protect minority groups. Policing bodies should make data on equality impacts of trial use of technologies publicly available. b) **Training to ensure awareness of equality and human rights obligations** should be given to all officers involved in the use or monitoring of emerging technologies. Force polices, guidance, and training (developed in accordance with EA2010 and PSED) may be used to inform officers and staff about ethical standards and the methods in which behaviour is compliant with bias mitigating efforts.

6. Consultation and public engagement

In this chapter an evidence-based approach to consultation and public engagement is outlined, based on the report of the third workstream of the IAG (Campbell et al., 2023). A range of literature, best practice and learning from experiences in Scottish policing and elsewhere was used to develop an evidence base and framework for consultation and engagement that sets out proposed principles and practice for clear, meaningful, accessible and appropriate approaches to engage on emerging technologies in policing.

Background:

As would be expected, given the Police and Fire Reform Scotland Act (2012) emphasises collaborative working and engagement with communities, policing bodies in Scotland are expected to work closely with stakeholders and the public in developing their approach to future service delivery. This includes a consideration of an understanding of the views of the public and a range of communities and stakeholders. Furthermore, appropriate consultation is a key requirement of the DPIA process (ICO website) and can help ensure that processing is fair (meets the public's reasonable expectations) and that potential risks are identified, assessed and appropriately mitigated. ICO guidance is that the views of individuals (or their representatives) should be sought unless there is a good reason not to.

Police Scotland has made efforts towards developing accessible, inclusive and meaningful approaches to public engagement, in order to improve policy and practice. The Strategy, Insight and Engagement service within Police Scotland is growing and supporting different approaches to insight, engagement and public participation – and it is their intention that the report of workstream 3 of the IAG will enhance this work across policing more generally, beyond emerging technologies. Their intention is to be led by research and best practice in order to make Police Scotland's public engagement process more robust and representative and inclusive of diverse communities.

Evidence and best practice:

A range of literature and evidence on best practice in consultation, engagement, deliberative and democratic approaches was reviewed by the workstream in order to draw out some considerations for policing. Engagement is seen as one way to support the police to build trust and confidence, with police legitimacy linked to the notion of 'policing by consent' seen as being central in a democratic society. Public engagement and participative approaches are seen to be important in understanding public expectations of policing and factors that shape public trust, confidence and legitimacy.

Participatory approaches to democracy seek to involve people in order to inform policy development and service delivery, with the intention being to meet the needs of the public. In order to be effective, the approach to engagement and participation should be tailored for different situations with a combination of tools used as part of an evolving approach within a framework underpinned by clear principles (Mistry, 2007 cited in Campbell et al. 2023). Deliberative processes seek to explore complex issues and can be used to weigh up trade-

offs. Deliberative processes are being encouraged in the UK in order to that decision-making is informed by what local people want.

It is important to acknowledge various dimensions of deliberative approaches: participation, influence and communication, and decision mode (Fung, 2006). There is an acknowledgement of limited evidence on best practice in how best to execute feedback to participants and communities and this should be explored with stakeholders when planning public engagement.

Learning from case studies:

It is important to note that engagement with the public is not binding and hence there is no mechanism to challenge a public body if the public's views are not taken into account appropriately. However, when formal consultation is used judicial review may be used to challenge the lawfulness of a decision made by a public service. Campbell et al. (2023) draw out learning from various examples where judicial review has been used in England and Wales, as these would be considered if a similar case were to be raised in Scotland. Some of the considerations arising from these include the fact that: the outcomes of consultations may be questioned if the 'option development' processes are flawed; there may be advantages to providing the opportunity to advocate solutions other than the stated ones; consultations should not be over-reliant on website/digital methods to reach people.

The creation of Social Security Scotland's Our Charter is highlighted as an approach which was underpinned by the Scottish Approach to Service Design and was developed *with* people to ensure as far as possible that services meet the needs of diverse communities and. It is accessible in a variety of formats and sets out in clear and accessible language the expectations that people should see within the social security system in Scotland.

The Scottish Community Engagement Standards (inclusion, support, planning, working together, methods, communication and impact) were recently refined (with stakeholders including Police Scotland) to help ensure that community engagement activity facilitated by organisations is deigned, delivered and evaluated in a way that is fair and effective and will increase participation and impact.

Citizens' Assemblies usually involve people who reflect the wider population and are reimbursed for their time (in order to reduce barriers to participation) and follow a process of learning about an issue and deliberation among members before decision-making. Research from the Citizens' Assembly of Scotland highlights learning on this important process. Citizens' Juries may be used as a smaller and less expensive form. Deliberative processes involve participants weighing up arguments and exploring trade-offs and these work best when there is no clear solution to a problem. They are time intensive and require skilled practitioners to be involved in design and delivery and people with subject expertise, as well as decision making power involved at key stages. Therefore, if this is not feasible then other methods of public engagement should be considered.

West Midlands Police's development of a predictive analysis system (National Data Analytics Solution) is drawn on by Campbell et al.(2023) as an example where, in addition to engagement with key stakeholders in relation to ethical and legal compliance, it would have been useful for police to undertake public and colleague engagement as part of developing new systems. This engagement would ideally take place at the earliest possible

stage of technological development, deliberating on why it is required and if it is being progressed then working with decision makers on options for implementation. In relation to public confidence it is important for the public, particularly individuals and communities who have negative experiences of views of the police, to understand what the police are using data for.

Democratic Society's use of a public engagement programme to inform the development of Scotland's Artificial intelligence (AI) Strategy provides learning about digital engagement, including providing honorariums and devices and mobile internet where necessary, and offering 1-1 sessions as well as online workshops.

The example of Police Scotland's introduction of digital triage devices 'Cyber Kiosks' and the Scottish Parliament's Justice Sub Committee on Policing's inquiry[25] highlighted that consultation with internal and external stakeholders prior to the implement of new policing policies or technology is best practice.

Police Scotland's engagement programme on BWV took that on board and engaged more widely, conducting two national surveys (with circa 9,000 responses each) and a series of 13 focus groups with diverse communities and those affected by crime. The results are being used to inform changes to planned service delivery in a manner which is more likely to receive public support. The learning for future engagement includes: independent review by stakeholders of supporting evidence and the opportunity for participants to engage with accessible materials in order for evidence to inform views before taking part (covered in chapter 3 on research); consideration of use of formal consultation (rather than engagement), which was introduced as an additional step and therefore subject to judicial review.

The engagement on BWV was further supported by the use of focus groups which sought to understand attitudes towards police use of technology to inform consideration at an early stage. Focus groups are helpful to enable greater understanding of views and concerns and they were also used to 'understand the factors which may lead to public support or non-support for the use of technology' (Campbell et al., 2023: 22).

The acknowledgement that police should be clear about the purpose of engagement comes across clearly in the workstream report. In my view as Chair, although the purpose of an engagement may be quite open, e.g. to understand public views, it may also be worth reflecting on how that information may then be used. For example, if the police plan to introduce a technology then they should be up front about that and not seek to engage in order to figure out what the best approach might be to 'foster acceptance'. Clearly engagement should seek to provide genuine unbiased understanding of the balance between risk and benefit and not seek to drive acceptance, but rather listen to concerns and take them into account in decision making about how, or indeed if, it should be implemented. It is important to consider what information (about police use of technologies) is provided to participants (see chapter 3).

The workstream 3 report highlights the following elements of good practice drawn out from the evidence base, case study assessment and public sector experience:

[25] Report on Police Scotland's proposal to introduce the use of digital device triage systems (cyber kiosks) | Scottish Parliament

- Public engagement should genuinely involve citizens and communities in open, two-way conversations on how best to tackle problems.
- The public, communities and colleagues should feel a clear purpose for the engagement has been shared, they have been listened to and that their needs will be considered.
- Approaches need to be adopted that are inclusive, representative and relevant to the public, communities and decision-makers.
- Decision-makers need meaningful and actionable insight that is outcome-focused and offers practical solutions to support operational policing design.
- Evidence and materials that support engagement must represent a range of views to enable an open and transparent dialogue. They must be accessible and inclusive for a range of needs such as producing 'easy read' versions of materials, and working with subject experts to understand any tensions, with any evidence being provided to inform decision-making.
- A safe and well facilitated environment for engagement where people can listen to others' views and opinions, with decision-makers also present and engaged in the process.

Understanding the reasons for engagement and clarity on the topic under review is crucial if meaningful engagement is to happen.

- This requires careful internal consideration of whether the process and those involved can actually influence the issue, policy or decision at hand in order to work out what is in scope at the outset i.e. how much the opinion of the public will be taken into account.
- Organisations must be honest with the public about what they can influence and how, what might happen as a result and when they can expect feedback (and ask participants of engagement what format would be most useful).
- Different engagement approaches must be considered for different needs (of decision makers and those whom the decision will affect).

Public engagement should be a continuous process and a range of methods can be used. Consideration should be given of when a *formal consultation* is required.

Participation and engagement framework:

Based on best practice, workstream 3 developed **principles for engagement** focused on a policing context. These may be found on page 27 of Campbell et al. (2023) and include *relevance, inclusivity and approachability* (accessible methods that enable two-way conversations, understanding cultures and sensitivities and doing things with those who are impacted); *transparency and accountability* (producing actionable outcome-focused insights and being honest about what is being done and why); and *innovation* (using co-creation with communities to turn problems and ideas into solutions and empowering and enabling communities).

Meaningful and effective engagement should involve dialogue, respect, integrity, transparency and accountability. It provides an opportunity for people to shape services and influence decisions and should be inclusive. Relational power dynamics policing processes should not exclude people who have had contact with police and may have engaged in criminal activity. Indeed in my view as Chair it is important to ensure that every effort is

made to engage with those who have been in contact with the police as suspects, not just victims, as well as members of the public who may not have had any interactions.

Emerging democratic practice highlights a range of best practices which may enable better outcomes:

- Shared community spaces for dialogue and communication;
- Open, visible safe space to identify problems, foster creative thinking and generation of ideas;
- Further engagement may be done through surveys, focus groups and workshops to test concepts, capture concerns and benefits from a wider audience;
- Citizen experience mapping and behavioural research may be used to understand interactions with technology;
- Citizens may work together with subject-matter experts towards developing recommendations, principles or other outputs.

Designing meaningful public engagement processes takes time, resources and expertise but not all engagement requires maximum use of resource to achieve quality outcomes and where resources are constrained some public engagement is better than none at all. Formal consultations with fixed timelines to determine the level of support share a limited level of decision-making with the public. The level of participation and methods to achieve the desired outcome require careful planning. Engagement can be ongoing and the level of participation and nature of involvement will depend on the purpose of the engagement. Police Scotland's adaptation of Arnstein's Ladder of participation runs from *inform* at the bottom to *review*, *discover*, *involve* to *empower* at the top and examples are provided (Campbell et al., 2023: 21). Careful consideration must be given to how much influence those involved can have in order to choose the right level of participation and ensure transparency of dialogue and the selection of the most appropriate methods.

Principles for accessible and inclusive engagement outlined include:

- Adapting the consultation or engagement process e.g. to ensure people impacted by disabilities or marginalisation can take part meaningfully;
- Ensuring the way engagement is done does not exclude people (take note of the Equality Act 2010 and engage with experts and lived experience to plan sessions and locations);
- Include people from diverse background in engagement in order to aid understanding of how people with different needs or abilities may be impacted, to shape the design, functionality or content of services and ensure you meet best practice guidance and legislative requirements to support equality, diversity and inclusion;
- Where possible go beyond the minimum standard expected and doing what is best for the people you want to involve and reviewing the approach regularly;
- Avoid stigma and making judgements and assumptions about people's needs;
- Involve all groups and ensure compliance with the Equality Act 2010 in relation to the rights of people with protected characteristics (age, disability, gender reassignment, marriage and civil partnership, pregnancy and maternity, race, religion or belief, sex, sexual orientation);
- Of note Police Scotland has a specific duty under the Equality Act to publish and report on progress relating to equality outcomes;

- It is important to acknowledge that children and young people are an integral part of communities and children have specific rights. They can also be involved in design of services and policies and various national and local structures, groups and organisations across Scotland can act as a conduit to engaging with children and young people. It is noted that Police Scotland have developed a team with expertise in facilitating high-quality engagement with children and young people. Also, the Children's Rights and Wellbeing Impact Assessment (CRWIA) is part of the suite of assessments to be considered in the planned sixth case process (chapter 8).

Ethical guidelines for engagement outlined include:

- Engagement and research should aim to maximise benefit for individuals and society and should be conducted with integrity, fairness and respect.
- The wellbeing, privacy and human rights of individuals and groups should be protected at all times.
- There is a responsibility to make sure the physical (e.g. consider safety, travel and risk assessments), social (e.g. consider impact on belonging to community), and psychological (consider sensitive topics and minimising distress) wellbeing of participants is not negatively affected.
- Participation in engagement activities should be based on freely given informed consent (requires clear explanation). Data must be processed in line with GDPR principles as (currently) contained within the Data Protection Act.
- Managing expectations of participants before, during and after the engagement process is vital, including acknowledging that not all public engagement activities will bring direct change or improvement in the lives of participants. It is important to be open and realistic about expected outcomes and influence of the activity and involve participants and decision makers from the start by exploring what success would look like for them.
- Feedback to participants is vital to ensure ethical practice;
- Senior leads should ensure that where appropriate and proportionate to the engagement a Data Protection Impact Assessment and Equality and Human Rights Impact assessment is in place to protect participants and mitigate risk.
- Additionally, in my view as Chair it would be worth reflecting on good practice in research ethics and integrity (informed consent etc.) and encouraging internal engagement and research carried out by Police Scotland (or other entities acting on their behalf) to adopt that guidance.

An engagement road map planning tool (Police Scotland website) has been created to support decision-makers and others involved in commissioning or leading public engagement to consider some of the critical components of high-quality engagement.

Police colleague engagement:

Findings from the Your Voice Matters survey suggested that Police Scotland should listen and gain a deeper understanding of the areas that matter to colleagues. This means involving colleagues in shaping how things are done in order to improve their experiences and in the co-creation and design of services that will help improve the safety of communities they serve. Indeed, experiences of police officers and their perceptions of organisational justice can impact how fairly the public are policed and police officers should be engaged with and involved in shaping changes at the outset in order to enhance their chances of success (Aston et al., 2021b).

Findings from the Your Voice Matters survey suggest that colleagues seek open and transparent ways to make suggestions to support continual improvements, they wish to be listened to and for their views to shape decision-making processes. A collaborative and open engagement approach will enhance the ability to engage in pro-active listening and involve colleagues in change management and sharing ideas for improvement at an early stage. Employee engagement is central to attracting and retaining talented workforce and Police Scotland hopes to build on their current initiatives (Chief's Forum, Truth to Power Sessions and Your leadership Matters) in order to enable the service to consider what everyone has to say, seek and share views and information in new ways, listen to one another's concerns in a collaborative and safe process regardless or rank and solve problems and make decisions together.

There are number of key areas relating to the introduction of technology on which to engage and involve colleagues e.g. protecting human rights; skills, knowledge and technology required to deliver service, and how colleagues feel about using emerging technologies. Colleague engagement should be a continuous and evolving process and feedback must be provided. Open two-way dialogue that is safe and inclusive and facilitates reciprocal exchange of ideas and feedback must be facilitated. It is important to involve and support colleagues in order to create a psychologically safe workplace environment and this is supported by Police Scotland's Values and Competency Framework and Code of Ethics (see figure p.40 Campbell et al. 2023).

Colleague engagement is key to organisational development and wellbeing and a number of suggestions are made to enhance this activity in Police Scotland including the introduction of an internal colleague engagement platform, focus groups and collaborative service design workshops.

Assessing and building participative approaches:

A range of new public engagement methods and tools are being developed and introduced by Police Scotland. An assessment of maturity of these practices in Police Scotland is provided by Campbell et al. (2023: 43-44) outlining areas which are: mature within the organisation (e.g. Citizen Space, Police Scotland Engagement Hub); new for Police Scotland but adopted by other public bodies and developing in policing (e.g. Reputation Tracker, Your Police: Community Conversations); those that are new for Police Scotland, breaking new ground in the public sector and aspirational for policing (e.g. Dialogue digital hub, Your Police Panel).

Chapter 6 summary and conclusion

This chapter has set out proposed principles and practice for clear, meaningful, evidence-based and appropriate approaches to consultation and engagement on emerging technologies in policing. At the heart of the framework is enabling genuine public dialogue and participation in order to influence change in policing. There is acknowledgement of the central consideration of legitimacy, trust and public confidence. Understanding the needs of Scotland's communities remains a top priority for policing in Scotland and therefore effective engagement is crucial. The Community Engagement Standards for Scotland support policing to deliver this.

Evidence-based principles for enabling meaningful engagement and consultation include:

- a bespoke design for each initiative underpinned by a clear purpose and principles, using a combination of tools;
- different engagement, consultation and deliberative approaches for different needs;
- consideration of the levels of engagement and participation and what is appropriate for different types of inquiry;
- application of shared values in engagement, doing things *with* rather than to/for stakeholders and understanding the impacts.

In conclusion, a number of key considerations relating to consultation and public engagement are outlined here (see Appendix C for full details).

6.1 Policing bodies should **ensure engagement and consultation considerations align effectively with both legal and governance frameworks, and consideration of ethics,** via an appropriate organisational model.

6.2 Policing bodies should be **clear on the purpose of the engagement process from the outset** – what people are going to influence, why and how.

6.3 Policing bodies should **engage at an early stage in the governance process to understand views and sub-groups where a greater understanding of concerns is needed.** This is critical for complex or less understood technology (such as AI and predictive analytics) and high-risk projects.

6.4 Policing bodies should include an **element of formal consultation in the approach to ensure that the views of the public and communities are both adequately considered and embedded at an appropriate point** for all new and emerging technology.

6.5 Policing bodies should set out to have an **ongoing dialogue with the public utilising participatory approaches where appropriate**, as the technology is considered and during/ after implementation. This will enable concerns, risks, and suggestions for improvement to be considered and addressed at all stages.

6.6 Policing bodies should use a **clear and transparent engagement framework underpinned by engagement principles and quality assurance to ensure the process is clear and well-articulated**. This will guide the design of engagement which can be tailored in terms of levels of participation and methods.

6.7 Policing bodies should ensure **all engagement and consultation processes are inclusive and accessible for everyone, including protected groups defined in the Equality Act 2010 and ensure representation from a variety of Scotland's communities**. This should occur at as early a stage as possible.

6.8 Policing bodies should enable the **colleague voice to be heard as a key element of shaping proposals.** An open two-way dialogue that is safe and inclusive, and facilitates a reciprocal exchange of ideas and feedback should identify problems or conflicts, and solutions to improve the quality of police-citizen interactions, as technology is introduced and embedded.

6.9 Policing bodies should ensure **engagement insights, providing a clear narrative of the views of the public and communities, are considered and scrutinised by governance bodies**. This must include areas of concern and how these are being balanced, addressed and mitigated.

6.10 Policing bodies should make a **public, open and transparent commitment to *how* the insights from the engagement process will be used to shape the consideration and implementation of new technology and also report back with details, which are made publicly available and scrutinised**. Clear routes should be provided for the public to provide feedback, raise concerns or suggest improvements.

6.11 Policing bodies must **communicate with the public and other stakeholders about police technology capabilities and substantial changes to the dynamic of police work mediated by technology**. **This communication must be clear, public facing and speak equitably to a broad range of publics.**

6.12 Policing bodies should **involve key stakeholders and members of the public in the formulation of police guidelines in the use of technologies** to involve them and provide understanding of the rules.

7. Technological innovation and scientific standards

This chapter explores barriers and facilitators to technological innovation and adoption; viewpoints of technology providers on the future horizon for technological innovation and requirements in relation to scientific standards. This includes looking at data driven innovation; the place of the needs of victims and others in technology adoption; data interoperability and standards; and a consideration of what next generation standards for digital evidence management may look like. This chapter is derived from the workstream 2 report (Buchanan et al., 2023).

Barriers and facilitators to innovation:

In this first section a summary is provided of an analysis of the barriers and facilitators to innovation conducted by Matthias Wienroth and Megan O'Neill (see chapter 3 of Buchanan et al., 2023), drawing on research in health and policing domains. They define technological innovation as referring to research, development and deployment of new devices, materials, equipment, but also of procedures and processes, including software, novel services and systems, and analysis approaches. Technological innovations need to be considered as part of wider socio-technical processes (Bijker, 1997). The concept of *adoption space* provides a lens through which to analyse how and why technologies may not be adopted into practice. The lens describes a dynamic spatial and temporal space, populated by human and non-human actors, where attitudes, practices, interactions and events, along with material features of technology, shape technology perceptions and how it is used (Ulucanlar et al., 2013).

Technological identities (Ulucanlar et al., 2013), or understandings of how a technology might work, are socially constructed and relate to novelty, effectiveness, utility, risks and requirements and shape the desirability, acceptability and adoptability of technologies. As the way that technologies are perceived by stakeholder groups contributes to their adoption or rejection in practice, there is a need to involve diverse stakeholder groups and understand the wider sociotechnical field of a technology in order to identify and approach barriers and facilitators for technological innovation.

MacNeil et al (2018) provide an account of barriers and facilitators of technology innovation in the health care system in Canada and propose six dimensions within which to analyse and address them: development, assessment, implementation, policy context, resources, and partnerships/communication. Critiquing a strong commercial on focus technology procurement and a siloed approach to innovation, they suggest a longer-term focus should be taken to innovation with an emphasis on value (contributions of technological innovations to achieving the goals and priorities of policy, users, and society to address user needs). A range of relevant barriers and facilitators are outlined and may be found on pages 16-17 of Buchanan et al. (2023).

At the *development* stage there should be an emphasis on being inclusive, meeting user needs, providing seed funding for innovation, raising awareness of needs among developers and providing opportunities for developers to consult with user groups in order for feedback to be incorporated. This is in addition to meeting regulatory requirements such as Data Protection by Design and Default. At the *implementation* phase there was an acknowledgement that short-term focus may prevent longer term gains; commercially focused competitive models of procurement focusing on cost-containment may disadvantage innovation; and block procurement may disadvantage smaller local developers. Instead, they recommend a move to value-based procurement with a focus on user outcomes over the life cycle of technologies; enhanced collaboration via risk-sharing and value-based pricing; developing metrics that consider societal impacts of technological innovations; enabling universities to be involved and hold IP; developing support materials for procurement and insights into how technology is transferred into practice. The *resources* dimension again highlights a focus on cost-containment and fee-for-service resource allocation as counterproductive and instead propose a value-based approach, identifying successful programmes to scale up, and tax credits for innovation. The *partnerships and communication* dimension highlights a range of issues including inconsistent consultation and inclusion of user and public views and needs, lack of signposting, lack of collaboration on understanding value, and lack of communication. They propose forming early partnerships across stakeholders, involving users in testing, forming partnerships to translate research into practice, and developing a collaborative environment with communication tools that enable trust, information sharing and understanding.

In the policing domain, Wienroth and O'Neill cite Laufs and Borrion (2021) who provide a practitioner-based analysis of key barriers and facilitators for technological innovation. If innovations have been shown to enhance efficiency and effectiveness in policing practices they are more likely to be adopted. Key barriers include: lack of interoperability with existing systems (within a force and with partner agencies); and lack of social acceptability (public and or practitioners). Practical impacts (e.g. workload, communication, reporting) are noted as significant burdens for technology adoption. Public-private partnerships are raised as an issue given that private developments may be beyond the control of police and can potentially interfere with policing needs. Political and financial commitments (in supporting the ecology to foster innovation in flexible and innovation-open structures with supportive leadership and clear innovation adoption guidelines) are emphasised as facilitators to innovation uptake.

Lessons for technology innovation in policing include the need to focus on the ecology including flexible structures and a strong institutional framework and sustainable innovation practices. Procurement practices and the availability of finance can be a key barrier to research and development for technology innovation. Within a system of block-procurement commercial providers may focus on low-cost technology developments which show quick results which may be to the detriment of a longer-term strategy of innovations and may in fact necessitate extra effort and funding over time to given the stop-start approach. An example is provided of the loss of the Forensic Science Service in 2012, which has led to the English and Welsh forensic DNA market losing its innovative edge. Procurement benefits from an analysis of needs and a longer-term perspective on which aims to pursue and which partnerships to develop.

Change in practice and culture: Leadership, organisational and financial support for development and implementation, training, clear guidelines and rules can facilitate

innovation. Evidencing the value of introducing innovations and involving users and stakeholders in decision-making, design, implementation and deployment of new technologies can facilitate their useful uptake into policing practice. Incompatibility of new and old systems, practices, devices etc. can be a significant barrier to innovation in practice. Whilst interoperability is often the ideal, function creep raises concerns e.g. the use of cross-database searches. Organizational structures and cultures play a key role in the adoption of technology into policing. The ways technologies have been developed may prevent certain uses or aspects (e.g. path dependency or lock-ins) so these must be clarified in conversation with diverse stakeholder groups during development and implementation phases.

Social acceptability: Whilst innovation may be easier to implement when existing technologies are taking on new forms or roles, when technological innovations enable enhanced or widened use of existing capabilities the development of further uses of technology and data, of interoperability between different systems and technologies may negatively affect their social acceptability. Therefore, engagement with wider stakeholder groups outside policing and policy is vital, particularly as prejudices and institutional bias can be translated into and proliferated by technological innovation, exacerbating inequality.

Technology providers views on innovation and standards:

Given techUK's involvement in the IAG, in order to represent the technology sector, this section summarises the findings of a call for evidence which went out to their 850 members and received 16 responses. This section is derived from Georgina Henley's input, chapter 4 of the workstream 2 report (Buchanan et al. 2023).

In response to techUK's question about how victims could be put at the centre of discussions around technological development a number of important points were raised.

- Challenge driven innovation is key -policing must focus on the challenges first and then how technology will solve it.
- Updating victim support services on technological developments in evidence preservation and sharing within policing and the wider Criminal Justice System (CJS), and how technology aids investigations, should allow them to support victims to better understand what may be asked of them and why by police, prosecution and defence.
- The speed at which officers and investigators can access relevant information on a case is critical to victim care. A comprehensive user-centred design (UCD) approach is advocated in order to navigate a complex and sensitive user landscape and understand user/victim needs e.g. understand why victims may withdraw, ensure victims can submit evidence from home and withdraw consent easily (however, it is noted that it depends what kind of consent is being referred to as data protection consent is problematic in a policing context).
- Digitising manual and repetitive functions (e.g. Cell Site Analysis Suite Communications Data Automated Normalisation) to increase operational efficiency may lead to successful and quicker resolution and improved victim satisfaction.
- In terms of data interoperability and data sharing there may be a need to access data from many unrelated systems therefore considerations should be given to: anticipated data flows and roles and relationships under data protection law to ensure that data flows are compliant; data repositories on collaborative platforms; accessible digital entry point to CJ/victim support with victim support groups consulted regarding design of digital solutions; access to data from unrelated systems (POLE, People Object Location

Event); sharing the experience of victims with technology companies to enhance understanding and risk of harm; improving data quality through training and a bottom-up approach towards next generation level data and defining a common data scheme across forces and wider public service.
- Training is essential, as is collaboration e.g. Scottish Government Digital Evidence Sharing Capability (DESC) (multi-agency data sharing throughout investigations and prosecutions).

In summary, to put the victim at the centre of technological developments there should be accessible digital entry point to CJ/victim support; data-linkage within Police Scotland and with partner agencies; input sought from victim support groups when designing digital solutions.

In relation to what next generation standards look like for data/digital evidence management a number of points were raised:
- With regards to poor quality datasets and their negative impacts the UK Government intends to outline standards for algorithmic transparency and standards for data foundations.
- European Commission's proposed Artificial Intelligence Act highlights the need for transparency, interpretability and confidentiality of high risk (policing) AI systems and stresses the need to understand the capabilities and limitations of AI systems, interprets the system's outputs as well as being to override, reverse or not use the AI output.
- The USA's National Security Commission highlighted that AI performance should be continually monitored, document sources and create procedures for human supervision.
- Data sharing: standards should outline processes that enable data to be shared (without a lot of administration) and cataloguing data and sharing business concept and repositories. Data Sharing Agreements should be in place setting out how data will be shared in compliance with the law (see ICO Statutory Data Sharing Code of Practice).
- Ease of process: standards which can be adapted to be machine readable to allow automated validation of data.
- Accuracy and compliance with legislation: next generation standards in presentation of data /digital evidence need to show fairness (available and accessible to prosecution and defence) and audit trail.
- Common language: next generation standards ought to seek common language to aid understanding across the UK.
- Interoperability: fully connected systems require uninterrupted integration and information flow among various systems. These need validations on ethical grounds (as some data may be unproven intelligence and lead to unfair use). Interoperability and integration within force and across partner organisations for seamless information flow and to enhance operational effectiveness. Clearly all this must be in compliance with data protection law –the fourth data protection principle (Section 38 DPA 2018 places a number of obligations on competent authorities in terms of accuracy, whether data relates to a victim, witness or suspect and a requirement to verify the quality of data before it is transmitted or made available (including providing information so the recipient can assess the degree of accuracy, completeness and reliability of the data).
- Improving data quality: force wide education about AI and ML systems and requirements of data; bottom-up approach to developing standards for next generation level data; definition of common data scheme.

- Digital data is likely to come under more scrutiny (large datasets may need to be obtained in order to extract a small amount data) as it becomes more central to investigations so evidential standards need to be brought up to speed.

In summary, next generation standards for data/digital evidence should be designed to: meet user needs in line with Digital Service Standard and Government Digital Service Standard; enable data interoperability within and between police organisations; conform to published specifications for storage, sharing and security ensuring a common understanding of 'what good looks like', improving the quality and utility of data and ensure compliance with DP Law and the ICO Data Sharing Code of Practice.

In terms of the standards industry should be aware of e.g. from outside policing the following were mentioned:

- ISO27001 looks at how to manage information security (avoiding human error, confidentiality and data integrity); ISO9001 looks at Quality Management standards (end user satisfaction). ISO27037 and ISO27041 regarding digital evidence.
- POLE standards to ensure these four critical aspects of data in policing when enabling interoperability of data and information between systems and forces.
- Pre-Cursor Policy and Legal constraints (audit of what, how when and by whom technology used and what the outcome was) with legal, user guidelines and local policies on use to maintain evidential sanctity.
- Digital Scotland Service Standard and Government Digital Service Standard for creating public services in a user-centred way.
- Gov.UK Data Ethics Framework (guidance on how to use data appropriately and responsibly when planning, implementing and evaluating a new policy or service)
- NHS digital, data and technology standards framework (clear standards for enabling better use of data).
- MAIT (Multi Agency Incident Transfer) standard provides ability for emergency services to securely share electronic incident records in DML reducing CAD information exchange time and allowing accuracy and timeliness of information allowing informed decision making with other agencies.
- Ensuring humans are present in and understand the AI governance chain in order that regulation and ethical considerations are adhered to
- Furthermore, the ICO Data Sharing Code of Practice and the ICO Children's Code may be relevant for services that do not fall in scope.

In relation to the question on evidence-based decision making and how the tech industry can engage with academia this is covered above in Chapter 3 of this final report.

Innovation and standards:

This section, derived from Bill Buchanan's input, i.e. chapter 5 of the workstream 2 report (Buchanan et al., 2023) covers some of the background around how innovation technology is currently handled and key areas of technological advancement. It highlights that many studies on adoption of technology in policing point to the need for strong leadership from both project leaders and police leaders in the roll-out, the centrality of sufficient training, the involvement with internal stakeholders and in understanding issues moral and ethical issues.

It is worth reflecting on what some of the top innovations (as ranked by police leaders) include: Combined DNA Index System (CODIS), Mobile data terminals (MDT); electronic fingerprint services, computer-aided dispatch, Automated Fingerprint Identification Systems, crime lab testing, next-generation 911, Body-worn video cameras, facial recognition, Facebook for PR, ariel drones /UAVs (Matusiak et al., 2020).

Lessons learned from a number of studies on innovation and the adoption of technology within policing are drawn out and include:

- Buy-in at frontline level and the need for specialised training and staff.
- The perception of the technology has a fundamental role in its adoption.
- Internal stakeholders should be involved in the planning process for a roll-out at an early stage.
- The use of technology in routine police practice depends on flexible and customized support from facilitating services, the motivation and perseverance of project leaders and police leaders, timely decision-making on project development, a clear organizational structure and governance, and overall police organizations need a clear innovation strategy and vision on technology.
- Resource-based view (RBV) may be useful in innovation and strategic planning.
- POLE (Person, Object, Location or Event) Standards are being developed by the Police Digital Service (Furuhaug, 2019) and Depeau (2022) outlines that graph technology could help considerably with the adoption of the POLE data model for crime data for use by police and other government agencies by generating relationships between various nodes. However, as Chair I note the important concerns raised in the earlier section by Wienroth and O'Neill regarding function creep (which should be considered and managed in a DPIA) and considerations on AI and big data innovations covered in Chapter 5.

MAIT standard provides the ability for emergency services to share electronic incident records securely in the form of XML. The improved accuracy and timeliness of information allows informed decision making when dealing with other agencies, freeing up time spent with callers.

The sharing of data by the general public with police needs to be handled with care. For example, the trustworthiness of data shared by the public on high situational severity crimes must be considered (Shore et al., 2022). In terms of crime prediction techniques based on big data hot spot identification models, near-repeat modelling; spatiotemporal analysis methods and risk terrain analysis may be used. However, there is a need to comply with data protection and equalities and human rights laws, as well as ensuring ethical standards and there is a lot of controversy around predictive policing using data and technology.

Furthermore, as Chair I would add that the United Nations Interregional Crime and Justice Research Institute (UNICRI), through its centre for AI and Robotics, and the International Criminal Police Organization (INTERPOL) are developing a Toolkit for Responsible AI Innovation in Law Enforcement. This is intended to fill a gap in the availability of guidance tailored to law enforcement on responsible development, deployment and use of AI and it will be a practical guide for law enforcement agencies worldwide on the use of AI in a trustworthy, lawful and responsible manner.

In conclusion, evolving standards (e.g. MAIT and POLE) could provide a foundation of future innovation. The use of technology in routine police practice depends on: flexible and

customized support from facilitating services; the motivation and perseverance of project leaders and police chiefs; clear organizational structure and governance; timely and fitting decision making on project development; and overall the police organization needs a clear innovation strategy and vision on technology.

Best practice concerning scientific standards:

Connon et al. (2023: 99-100) also cover research and police practice evidence on scientific standards for emerging technologies, with the literature focusing on AI. Ernst et al. (2021) recommend the development of a *vision on technology and innovation* and Storm (2017) found that there is a need for *technological guidance and a national technology clearing house* in the US would assist with avoiding the purchase of technologies with high probability of failure.

Oswald (2019) discusses the importance of scientific validity, drawing on evidence from the West Midlands context to demonstrate the need to consider *statistical and scientific validity* of the use of proposed technologies. Oswald points out that the development of policing algorithms is often not underpinned by robust empirical evidence regarding scientific validity and claims of predictive accuracy are often misjudged or misinterpreted, which makes it difficult to assess the actual impact of technology in practice. She recommends *context-specific evaluation methodologies for statistical algorithms* used by police forces which should include guidance on how confidence levels and error rates should be established communicated and evaluated. Also, clear scientific standards written with the police context in mind should be required for a national ethics approach.

Chapter 7 summary and conclusion:

Police organisations need a *clear innovation strategy and vision on technology*. The effective use of technology often depends on *flexible and customized support* from facilitating services; the *motivation and perseverance of project and police leaders*; *timely decision-making on project development*; and a *clear organisational structure and governance*. Technology innovation requires *sociotechnical change, including cultural change in practice, institutions and oversight.* Successful adoption into practice needs to *take into consideration user and stakeholder perceptions, existing systems and practices* at practitioner, policy and oversight levels and a variety of other elements that may be impacted on and are likely to have to innovate at the same time. Technological innovation should adopt a *value-based approach* and be a *longer-term process*. This means that decisions about procurement, replacing systems and changing practices need to focus on outcomes and establishing understanding and the willingness to experiment e.g. in small-scale test-runs. It is noted that where appropriate such experiments could be used, for example, to test different solutions or understand impacts in a controlled space prior to potential wider roll-out. Tests of change should be time bound with clear objectives and a transparent review process and at a minimum would require impact assessments at the outset. *Partnerships* are important for technological innovation and can strengthen the capacity for socio-technical change, encourage benefits to arise from such change and render innovation more socially acceptable.

As new technologies are developed it is important to put the needs of members of the public, particularly those who come in contact with the police (victims, witnesses and accused as well as complainants) *at the centre of an innovation* in order that there is a better understanding e.g. of touchpoints during an investigation. *Next generation standards should be designed to meet the needs of the user and enable interoperability* within and between forces to reduce cost, risk and complexity and conform to published specifications for storage, sharing and security (and allow for compliance with data protection law) and ensure a common understanding of what good looks like. Standards must be designed to meet the needs of the user in line with the Digital Scotland Service Standard and Government Digital Service Standard. The Public Sector Equality Duty provides a framework for ensuring that people are not digitally excluded, and that potential barriers to accessing services are mitigated against. *Police should integrate with developing standards including from outside of policing.* Various standards should be considered e.g.: POLE standards in enabling interoperability, ISO27001 which looks at how to manage information security and ensuring staff know how to manage data properly, Gov.UK Technology Code of Practice, Gov.UK Data Ethics Framework, and the NHS Digital, data and technology standards framework and the ICO's Children's Code and Data Sharing Code of Practice.

7.1 In order to facilitate successful adoption into practice, policing bodies should **prepare an implementation plan which assesses and takes into consideration stakeholder perceptions, existing systems and practices at practitioner, policy and oversight levels**.

7.2 Technology innovation is a longer-term process. In relation to decisions about procurement, replacing systems or changes to practice, policing bodies should focus on **establishing understanding and the willingness to experiment** e.g. in small-scale test-runs.

7.3 Organisations in the policing system and their partners should **invest in developing stable, longer-term mutual collaboration between industry, academia and public organisations**.

7.4 Policing bodies should **adopt next generation standards designed to meet the needs of the user and enable interoperability** within and between forces to reduce cost, risk and complexity and **conform to published specifications for storage, sharing and security and ensure a common understanding of what good looks like**.

7.5 Policing bodies should **establish a national technology clearing house to ensure robust scientific standards for AI technologies.**

8. Oversight, scrutiny and review

This chapter is derived from the IAG's workstream 4 report (Ross et al., 2023) and provides an overview of the existing decision making, oversight and scrutiny framework that is in place to support the assessment of the potential adoption of new technology across the policing system in Scotland. It also highlights recent steps to bring improvements and proposes further potential routes to enhancement. It follows the consideration and decision-making pathway of technology adoption from initial concept assessment, case for change development, decision making, governance approvals, project delivery and into business-as-usual adoption.

Introduction:

There is an acknowledgement that the legitimacy of policing in Scotland is connected to the principle of policing by consent, which is shaped by how legal, explainable, justifiable, and proportionate the decisions made by the Police Service of Scotland are deemed to be. This is subject to oversight, with a focus on the public interest, by the Scottish Police Authority, and a number of other bodies, including for example His Majesty's Inspectorate of Constabulary Scotland, Audit Scotland, the Information Commissioner's Office, Scottish Biometrics Commissioner and the Lord Advocate.[26]

It is acknowledged that ambiguity and uncertainty will often feature when considering the deployment of emerging technologies in policing. Therefore, assessing the available evidence, identified risks and mitigations and ensuring transparency will contribute to an informed assessment of the probable benefits and dis-benefits associated with the potential implementation of new and emerging technologies.

In justifying decisions and making them explainable, the policing system must be able to demonstrate that it has taken into account legal, ethical and human rights considerations in arriving at those decisions, taking into account the rights of the individual and the need to protect all citizens in their communities. This must be assessed (through the DPIA and EQHRIA) when considering proposals for the adoption of new technologies which aim to assist policing in its primary function of ensuring safety and wellbeing. Whilst the language of balance is often used in this context by policing bodies, IAG members discussed how certain things cannot be balanced or traded off against others, e.g. in the equalities sphere.

Ross et al. (2023) argue that there should be an avoidance on a overemphasis on the 'precautionary principal', i.e. not favouring change or innovation when there is uncertain evidence and small potential for future harm, as a basis for decisions in the face of uncertainty. Sunstein's (2005) definition however, emphasises that a small risk of harm would be catastrophic if it occurred. Ross et al. (2023) argue that whilst decision makers should have regard to the precautionary principle, instead the introduction of emerging

[26] Criminal Procedure (S) Act 1995, section 12
Police and Fire Reform (S) Act 2012, section 17(3)(b)
R v. Manchester Stipendiary Magistrates ex parte Granada Television [2001] 1 AC 300,305B-F'

technology in policing should be guided by the 'proportionality principle' when considering a public interest assessment of a proposed new technology or deployment.

The 'proportionality principle' is based on what is legal, legitimate and democratic, but is also cognisant that many operational policing scenarios involve the need to carefully balance the rights of individuals and assessments of threat, risk and harm. Decision makers should have regard for the following:

1) Intended purpose and benefits (under S32 of Police and Fire Reform Scotland Act) regarding the duty to improve the safety and wellbeing of individuals and communities.
2) Lawfulness and regulatory compliance, with particular regard to intrusion into citizens' privacy and private lives (through a DPIA and EQHRIA); open and transparent debate.
3) Balance of evidence of future benefits /harm prevented and future dis-benefit or harm caused. A 'public interest' approach to protecting safety and wellbeing and preventing harm while preserving individual civil and human rights.
4) Affordability and best value.
5) Planning of mitigating actions to reduce potential harms.

Police Scotland and the Scottish Police Authority have published a memorandum of understanding that outlines the principles through which decision making (including on the introduction of emerging technologies) and engagement will be conducted. There has been a great deal of progress since 2019 to establish robust processes and mechanisms to underpin this ethos. Indeed, His Majesty's Inspectorate of Constabulary (HMICS), have stated[27] that the governance arrangements are continuing to mature and evolve.

Overview of existing governance and assurance framework:

Figure 1 (Ross et al., 2023: 6) outlines the programme and project lifecycle process, which a proposal would follow in Police Scotland (it would be similar in SPA Forensic Services) as it develops: from initial concept assessment, to case for change development, informing decision making, followed by governance approvals, and through to project delivery and transition into Business as Usual.

As Chair I note that it mentions a range of organisations which may potentially be engaged with during this process, though whilst there is no obligation to engage with many of them, some of them, e.g. various boards mentioned represent key steps in the process. It would be worthwhile to highlight which steps or organisations are required to be engaged and which are not. Based on input provided by Dr Genevieve Lennon, it is important that the SPA should, independently of Police Scotland, obtain a technological assessment of the new practice or technology. There are a range of organisations listed, some of whom must be notified and consulted at the earliest stages (e.g. for new technology with some impact of biometrics, the Scottish Biometrics Commissioner should be involved from the outset). The requirement rather than option to consult ensures independence, a key principle for accountability (Lennon and Fyfe, 2022). Further, there should be sufficient resources to enable the independent bodies to best function, e.g., discretionary funding for the SPA, HMICS, PIRC and other oversight bodies to ensure they get an independent explanation of the emerging technology, independent of Police Scotland.

[27] HMICS | HMICS Assurance validation of Police Scotland transformation benefits 2020-21

Memorandum of understanding:

In 2021 Police Scotland and the SPA jointly developed a Memorandum of Understanding - SPA website) (MoU) which aims to ensure early visibility and oversight of any new and emerging strategy, policy or practice under consideration by Police Scotland or SPA Forensic Services that is likely to be of significant public interest. This is a step forward as previously only cases for change beyond a certain financial threshold would be presented to the SPA for consideration. It is underpinned by the overarching principles of early engagement and communication. This is in line with the statutory duty to work collaboratively with partners and in a manner that is accessible and engaged with local communities. The joint objective is to generate early and transparent public discussion and engagement on the issue and inform decision-making.

The MoU focuses on significant equalities, human rights, privacy or ethical concerns raised, or where the issue will have a significant impact on public perceptions of policing. It is also seeks to ensure that the intended benefits of proposed changes are clearly laid out and technological adoption improves the ability of policing to address threat, risk and harm.

The MoU also aims to ensure people's rights are considered and there is sufficient engagement with stakeholders and the public to inform the development in question. It provides opportunities for public discussion, local engagement and formal oversight and review. An early assessment and prioritisation approach is there to ensure innovations are planned and trialled in an engaging and inclusive way which considered a wide range of views and opinions in order to inform decision making on robust and transparent impact assessments.

The MoU involves the following stages: identification and assessment (with a strong focus on key ethical, privacy or human rights considerations); and communication, engagement and delivery. There is a stated focus on testing ethical, privacy and human rights issues; an engagement and communications plan to work with key stakeholders, the public and staff; full and transparent discussion; and informed decision making. There is also mention of use of best available evidence, consideration of testing with potential evaluation prior to full implementation, and a baseline and post-implementation review process to evaluate the impact delivered and any organisational learning.

SPA excellence framework:

It is acknowledged that effective scrutiny and oversight are key elements in ensuring that the public have trust and confidence in policing. The SPA Excellence Framework is part of the SPA's overall Governance Framework and it provides a conceptual structure intended to guide the development of Audit, Risk and Assurance Programme to deliver excellence within SPA and assurance around excellence within Scottish policing. In this context 'excellence' is said to involve ensuring organisations have a clear understanding of their stakeholders, develop ways to achieve or exceed expectations. achieve excellent results and communicate assurance effectively. The 'Four Lines of Defence' model (see diagram Ross et al., 2023: 9) is a core component of the Excellence Framework.

The assurance at the first line of defence (management) is provided by staff and management within or managing operations at divisional or functional level using business as usual activities such as good policy, performance data, risk registers, DPIAs, reports and

other management information. Whilst functional teams have ownership, responsibility and accountability for controlling and mitigating risks and this level of assurance provides an indication that performance is being monitored, this level lacks independence and objectivity.

At the second line of defence (oversight function) assurance is still within-organisation, but is provided by those separate from delivery and independent of the management chain, i.e. Police Scotland's Risk, Assurance and Inspection Team, Data Protection Officers (statutory role) and the SPA's Audit Committee. This line of defence monitors and facilitates the effective implementation of the first line of defence activity.

The third line of defence (independent internal audit) involves the SPA appointing independent internal auditors to report to the SPA's Audit Committee on how well the organisation assesses and manages its risks, including a review the first and second lines of defence.

In this context the fourth line of defence (external audit inspection and review) involves an independent assessment of the first three lines of defence and is undertaken primarily by external bodies including HMICS, Audit Scotland, the Police Investigations Review Commissioner, the Investigatory Powers Commissioner's Office (IPCO), the Information Commissioner's Office, local authorities and at a secondary level by the parliamentary Justice Committee, the Scottish Human Rights Commission and other regulatory/inspectorate bodies that oversee corporate bodies e.g. the Health and Safety Executive, See figure 2 for more information (Ross et al., 2023: 11).

Decision making, governance, oversight and scrutiny:

Although there is no specific board in Police Scotland or the SPA that considers emerging technology or ethics alone, many of the boards mentioned that have a role to play may be found in figure 3 (Ross et al., 2023: 12). As covered in Chapter 3, the potential governance route for new and emerging technology (see figure 4) involves six of the most relevant boards and relevant aspects of their role and remit are laid out on pages 13-14 (Ross et al. 2023).

Initial concept assessment:

As mentioned in Chapter 3, when a new concept or potential project arises, a Project Potential Assessment (PPA) template is completed in order to assess whether or not an idea is a Programme, Project, Business as Usual, Continuous Improvement or Small Change activity. It covers topics such as potential benefits, risks, impact on the organisation and costs/resources. The PPA is submitted to an internal Project board, Programme Board and then Portfolio Management Group. The PMG is an internal forum where the Senior Responsible Owner, Programme Mangers, Project Managers and Change Staff give approval, challenge and appraise papers and business cases. Data Protection Officers are also integral here.

Existing evidence from a range of sources (e.g. SPA/PS Joint Research and Evidence Forum, SIPR, SG Policy Advisors, College of Policing, PIRC, HMICS etc.) may be used to inform the PPA. Also, available information may be drawn together from internal engagements (e.g. Police Scotland regional and national ethics panels) or involving

external agencies (e.g. advice from reference groups), partners and regulators like SBC and ICO (e.g. on impact assessments) and potentially the public (e.g. public service polling).

Case for change development and informing decision making:

Both of these stages are connected and lead to the creation of the Initial Business Case. Its purpose is to begin exploring various options of how an idea could be delivered, and to assess the ethical, human rights, data privacy and compliance with DP law, equalities and other impacts of the proposed idea. Some of the areas it focuses on include high-level benefits and risks to the organisation that the project helps manage, impact assessment, dependencies, lessons learned, cost and resources needed for the next stage. The IBC goes to the Project Board, Programme Board, Police Scotland internal quality assurance, Portfolio Management Group, Change Board and Senior Leadership Board internally, before being presented to the SPA Resources Committee. Note senior staff who attend boards will keep the Data Protection Officer (DPO) cited.

There are clear expectations that output from internal and external engagement undertaken by Police Scotland should be incorporated into the IBC. This would include engagement with SG Police Division; assessed previous evaluations, potential test of change/pilot; Design consideration, EqHRIA and DPIAs, assessment through the Data Ethics Framework and consideration through Ethics Advisory Panels. The concept *could* be discussed through joint PS and SPA activity e.g. at joint evidence and research forum, legal opinion, SIPR and academia and other stakeholder engagement mentioned in the previous step. Similarly external agency, partner and public input may also include Independent Ethics Panels, Local Authority Scrutiny Convenors, Information Commissioner's Office, Human Rights Commissioner, Children and Young People's Commissioner, Scottish Police Federation and association of Police Superintendents. Input could also be gathered from frontline officers which would be important in terms of demonstrating an organisationally just approach and supporting meaningful organisational change (Aston et al., 2021b).

Governance and approvals:

This stage involves the SPA seeking assurance and evidence that the appropriate engagement has been undertaken with external agencies, public sector organisations, partners and the public as appropriate and research and an evidence base is presented to the SPA in the Full Business Case in order that they can make a decision on funding a project. The FBC should detail the engagement and advice given and what impact or substantial changes have been made to the proposed approach. Its purpose is to develop the options identified in the IBC and recommend a preferred option for the governance board to consider. The FBC is based on the UK Government project management guidance document The Green Book. This Five Case Business Model covered: the Strategic, Economic, Financial, Commercial and Management Case. The FBC should be accompanied by key assurance documents including Impact Assessments, Project Management plan, Benefits Realisation Plan and Risk Register.

The FBC goes through internal PS governance (approval at Project Board, Programme Board, Portfolio Management group, Change Board, Senior Leadership Board.). It then goes for external approval at the SPA Resource Committee, SPA Authority Board and SG if required. The SPA should ensure the appropriate impact assessments have been

undertaken, the previous steps of initial concept design, case for change development and informing decision making have undertaken the appropriate engagement, input and assurance from key stakeholders, subject matter expects and the public; and appropriate consideration has been given to equalities, human rights, privacy or ethical concerns raised. When SPA officers are briefing SPA board members they seek to highlight good practice, gaps or areas of concern in the FBC, in order to enhance scrutiny and requests for additional information. Therefore, scrutiny would be strengthened by inviting subject matter experts or representatives from professional reference or advisory panels to provide evidence or advice to members on the impact that an emerging technology may have on society, in order to inform their consideration of proposals.

Project delivery:

During this phase the project is subject to Change Control Processes and has to report to the Project Board, Programme Board, Portfolio Management Group, Change Board and Senior Leadership Board *if* certain thresholds are reached (e.g. 10% overspend). The project *may* be subject to an external reference group with independent external advisors which offers guidance to Police Scotland on delivery. The project *could* also be subject to SG Gateway Revises and SG Technical Assurance framework reviews, conducted by individuals independent of Police Scotland who would offer red, amber and green states on a number of categories including cost, benefit, resource, timescale or increasing risk. The project *should* still be engaging with external experts and regulators, the public and academia where appropriate in the design and implementation of the technology to ensure equalities, human rights, privacy or ethical concerns raised are being addressed. However, in my view as Chair, at a minimum engagement with external experts should continue during the project delivery phase, particularly for high-risk projects, or emerging technologies with a limited evidence base (and an evaluation of its implementation should be strongly considered). Novel projects that have mitigated risks at the outset should have continued monitoring and oversight.

Transition into business as usual:

A number of boards and performance reporting mechanisms *could* assess the impact that a project is having on service delivery. This may be done internally via PS boards (e.g. Local Policing Board, Operational Delivery Board, Senior Leadership Board). It may also be monitored through external groups and agencies including SPA (Internal Audit, Audit Risk and Assurance Committee, Policing Performance Committee, SPA Oversight Groups, SPA Board), HMICS Inspection, local scrutiny convenors, public survey and polling (by Police Scotland and or SPA) and Justice Committee.

The SPA should continue to require assurance that external evidence and advice has been sought and considered and that engagement with partners and the public has been undertaken to inform the approach to embedding specific technologies in policing and that risks and measures to mitigate risks are monitored and implemented. In my view as Chair, consideration should be given to routine collection of data (for research purposes and where possible made public to enhance transparency) on the impact (on various possible intended outcomes and unintended consequences) of the use of emerging technologies, particularly for high-risk projects, or emerging technologies with a limited evidence base (and an evaluation of its impact should be strongly considered).

Ethics panels:

In addition to the formal governance channels outlined above, Police Scotland have introduced four tiers of Ethics Advisory Panels (EAPs), which provide an opportunity for staff, officers, and external participants to discuss ethical dilemmas. The ethics panels are not decision-making bodies but provide advice and support to the decision maker (or dilemma holder), who remains responsible for taking the decisions, with due consideration of the panel's views in their rationale. For more information see chapter 5.

Additional oversight 1 – Scottish government, Parliament and HMICS:

The Scottish Police Authority is accountable (for its activities and use of resources) to Scottish Minsters, who are in turn accountable to the Scottish Parliament. The SPA must comply with any direction given by Scottish Minsters and the SPA Chief Executive is answerable to the Scottish Parliament for the exercise of their functions. The Scottish Parliament (in practice most scrutiny is through the Criminal Justice Committee) is responsible for scrutinising policy and legislative proposals of the Scottish Government. The Justice Sub-Committee on Policing was established to consider the operation of the Police and Fire Reform Scotland Act (2012), and it had a significant focus on new and emerging technology in policing (RPAS, BWV, Digital Triage devices, Facial recognition) but it was discontinued in 2021.

HMICS has powers to look into the 'state, effectiveness and efficiency of Police Scotland' and the Chief Constable must provide inspectors of constabulary with assistance and cooperation for the purpose of carrying out their function. These powers allow HMICS to investigate the effectiveness of the use of new and emerging technologies if deemed appropriate. However, it is more likely that HMICS will look at the service that the technology implementation will impact and take a view from an outcome perspective of whether the new/emergent technology has improved the delivery of policing, has delivered against the benefits from the business case and is compliant with law and ethical standards. Whilst the scrutiny plan for HMICS does not define any consideration of a technology implementation in its own right, as this is seen to be too narrow a focus, HMICS is83ifecyclg a Cyber inspection within the next two years and is likely to look at issues around the delivery of new technology with an operational and best value lens.

Additional oversight 2 – For example, SBC, ICO, Police Investigations and Review Commissioner, Human Rights Commissioner, Audit Scotland, Children and Young People Commissioner:

Emerging technology is likely to engage a number of areas already overseen by independent bodies. For example, data is likely to engage the ICO (regulatory scrutiny), while data of a biometric nature will engage the Scottish Biometrics Commissioner. The role of PIRC is to provide independent oversight, investigating incidents involving the police and reviewing the way the police handle complaints from the public. Audit Scotland provide independent assurance that public money is spent properly, efficiently and effectively and they report annually on the performance, governance and finances of SPA and Police Scotland. At the UK level there is also the Investigatory Powers Commissioner's Office which provides independent oversight and authorisation of the use of investigatory powers by intelligence agencies, police forces and other public authorities. Furthermore, there is

the Surveillance Camera Commissioner, Forensic Science Regulator and a range of other biometrics and forensics ethics groups and strategy boards which may be of relevance.

As analysis from Dr Genevieve Lennon outlines, oversight bodies may struggle to fully comprehend the nature or function of emerging technology. To ensure their independence it is necessary that they are appropriately resourced to meet this need, for example funded to hire a non-Police Scotland technical advisor to explain the technology, including likely benefits and costs (see Principle 2: Independence in Lennon and Fyfe, 2022). There should also be calculation of the likely impact on their independent bodies' roles, with resources adjusted as needed (e.g., a new, routine biometric practice could put substantial strain on the Biometrics Commissioner and require additional staffing).

It may be that these bodies identify costs in practice when the project is rolled out. While some may instigate their own investigations, others cannot (e.g., PIRC). Being able to launch an investigation themselves is particularly important in relation to emerging technologies that people may not be aware they are subject to (see Principle 3: compellability, Lennon and Fyfe, 2022). The power to instigate an investigation would require legislative change.

Rapid technological change can lead to the ossification of Codes of Practice (Kleinig 1996). All independent bodies, as well as the SPA and Police Scotland, should reflect on their codes of practice and comparable regulations in light of the adoption of new practices or technologies.

Finally, the 12 Principles of Accountable Policing outlined by Lennon and Fyfe (2022) provide a useful basis for enhancing oversight, scrutiny and review. These cover: *Universality* (covering the whole system); *Independence* (oversight bodies should not be dependent on the police for resources); *Compellability* (power to compel to provide information); *Enforceability and redress* (means to enforce and monitor progress); *Legality* (accountable to law); *Constructiveness* (dialogic process with feedback loop); *Clarity* (of oversight, expectations, expression and data); *Transparency* (provide accurate relevant timely information and public data on performance); *Pluralism and multi-level participation* (combination of democratic processes and consultative forums); *'Recognition' and 'Reason'* (pubic deliberation); *Commit to Robust Evidence and Independent Evaluation* (evidence and evaluation to guide decision making and deliberations of oversight bodies); *Be a Learning Organisation* (modifying behaviour to reflect new knowledge and insights).

Additional oversight 3 – policing and oversight bodies in other countries:

Effective oversight requires a feed-back loop, for learning and good practice. In addition to the Scottish organisations listed above, the police and SPA should ensure shared learning with other forces and oversight bodies, including England/Wales and Northern Ireland, as well as beyond the UK, and establish a learning loop from those bodies also. This is particularly important with emerging technology where there may be limited data on its use and impacts.

As Chair I would also note that with regard to strengthening accountability, lessons can be learned from other jurisdictions and the literature, some of which were drawn out earlier (particularly in chapters 4 and 5). Furthermore, useful insights come from accountability principles that have been researched and developed for specific technologies. For example,

building on Lennon and Fyfe's principles (2022), the empirically verified AP4AI Principles (Akhgar et al., 2022: 64) define requirements to be fulfilled to ensure Accountability for AI utilisation. The principles include: *Legality* (lawful plus where any gaps in the law exist, the protection and promotion of fundamental rights and freedoms should prevail); *Enforceability and Redress* (requiring independent and effective oversight and mechanisms to respond to instances of non-compliance); *Universality* (covering all processes, design, development and supply, use etc., in the AI lifecycle); *Compellability* (formal obligations from competent authorities and oversight bodies to compel those deploying or utilising AI to provide access to necessary information/systems); *Pluralism* (oversight to involve all relevant stakeholders engaged in and affected by AI); *Explainability* (information about use to be accessible and easily understood); *Transparency* (making available clear, accurate and meaningful information about AI processes and deployment to make informed judgements); *Constructiveness* (constructive dialogue with relevant stakeholders); *Independence* (of competent authorities performing oversight and in avoiding any conflict of interest); C*onduct*, (principles, professional standards and expected behaviours in a role, including integrity and ethical considerations); *Commitment to Robust Evidence* (requiring detailed, accurate and up to date record-keeping); and *Learning Organisation* (willingness to apply new knowledge and insights to bring improvements).

Part 2 ensuring ethical considerations are central to decision making in Scotland's policing system:

The need for innovation and technological adoption in policing is clear but this cannot be based purely on value for money -decisions must be made with the highest possible regard for ethical standards. The decision-making process in place has been outlined above, but through the work of workstream 4 of the IAG there was a recognition that there was an opportunity to ensure that ethical considerations are at the heart of the decision making by formalising the process. The approach should make use of a range of existing tools that can be applied proportionately to provide clarity in supporting the decision-making process. It should be flexible, scalable and provide a clear audit train in order to fulfil public accountability.

A sixth case model – the ethics and human rights case:

The Five Case Model outlined earlier in this chapter provides limited opportunity within it to assess the ethical implications of a project business case. It is therefore recommended that the present framework be enhanced to enable it to assist in determining, evaluating and balancing the ethical impacts of a business case. This would introduce a sixth case: the Ethical Case. This would consider the impact of change on a variety of aspects of ethics including human rights, the impact on individuals, society and on public confidence.

It is suggested that the use of the 'sixth case' should be proportionate so an independent triage process could be introduced to understand whether there are ethical implications that need to be discussed and addressed, thereby focusing resources towards areas of higher risk. A proposal to triage issues relating to data ethics across the policing system is presented in the next section on the Data Ethics Framework. Therefore, the SPA and Police Scotland should continue to develop a wider framework which sets out a systematic process for all ethical considerations, this should serve to guide the creation of a sixth ethics and human rights case which would be included in the Initial and Full Business

Cases. For Draft proposals for Oversight of Ethical Considerations in Policing see Appendix 3 in Ross et al. (2023).

Data ethics governance framework:

Following the establishment of the IAG, Police Scotland have developed a data ethics framework (introduced in chapter 5), which sets out how policing should cover its development and deployment of data-driven technology. It proposes new checks and governance tools be embedded into existing change processes and internal and independent advice will be sought to ensure the adoption of new technologies is proportionate, ethically justifiable and aligned with Police Scotland and the SPA's commitment to policing by consent. Policing bodies should implement the Data Ethics Framework across the policing system continues and that an effectiveness review should be undertaken 12 months after the roll out to ascertain the benefits realised and lessons learned during implementation.

The data ethics framework will provide the governance required to identify and address ethical challenges posed by novel uses of data and data-driven technology and guide its responsible use (and will provide valuable input into the DPIA). As outlined in chapter 5 the responses provided to framework questions relating to value and impact, effectiveness and accuracy, necessity and proportionality, transparency and explainability, and reliability and security should be open to internal and external scrutiny.

Although its focus is on data and data-driven technology, the methods and use of the sixth case approach can be applied to technologies that have limited or no data collection elements. Furthermore, it is proposed that the Data Ethics Framework provides a methodology and mechanism to ensure that the goals of the aforementioned Memorandum of Understanding in relation to data ethics are implemented in a consistent and repeatable way, and indeed can be used to cover a wider consideration of equality and human rights issues (see Appendix 3 in Ross et al., 2023).

The framework sets out how the policing system in Scotland should govern its use of data and data-driven technology and outlines mechanisms for internal input and how independent advice can inform decision making. The framework states that clear, robust governance arrangements should be established before investing in emerging technologies. In this case good governance is said to mean: establishing robust mechanisms for input (internal input/ challenge and external advice on decision-making - including proper understanding and weighing up of risks and harms); establishing clear responsibility and accountability (identifying key decision makers and decision points along the86ifecyclee); putting in place repeatable processes to identify, address and test ethical considerations and ensure consistency of approach and auditability. It is anticipated that as well as enhancing governance the framework will contribute to building public confidence and bring several other positive improvements (see chapter 5).

The proposed steps involved in the ethics governance framework include (see diagram in Ross et al., 2023: 31):

1. Ethics Advisory Panels discuss whether data-driven technology *should* be developed, ethical challenges, mitigations (at Problem Identification Stage)
2. Data Ethics Assessment (to be completed at planning stage) -to be embedded into IBC/FBC and DPIA

3. Digital & Data Design Authority (input at design stage), Data Ethics Oversight Group (internal input and oversight through project lifecycle -should include DPO)
4. Data Ethics Triage (determine whether additional internal/external scrutiny required)
5. Internal scrutiny (for high-risk projects during delivery stage. Data ethics toolkit used to identify and mitigate risks) -new internal Data Ethics Oversight Group required.
6. Independent scrutiny (again for high-risk projects during delivery and use toolkit) - new Independent Data Ethics Scrutiny Group required.
7. Ongoing Review (post-deployment monitoring)

Triage of risk -data ethics risk assessment:

In order to ensure that the highest risk projects receive the most oversight, the Data Ethics Governance Framework contains a set of eleven common triage questions to be used when considering a new project. The questions cover several dimensions including the scale and breadth of the project, the data being used, the outcome/effects, and potential disproportionality (for more information see Appendix 2 in Ross et al., 2023). Those identified as high risk through triage go through a detailed framework process, ensuring effort is focused on them.

Best practice and benchmarking:

Police Scotland have been mindful of aligning the development of the Data Ethics Governance Framework with some of the best practice in UK policing. They have drawn on the experience and learning from West Midlands Ethics Committee, for example, by including an independent external consideration and advisory. It is recommended that Scottish policing system continues to share experience with partner agencies nationally and internationally and share lessons learned in order to refine approaches.

In conclusion, it is suggested that Police Scotland continue to adopt their Data Ethics Framework and implement its key aspects including:

1. Data Ethics Triage for all new projects submissions;
2. Internal Scrutiny -set up an internal Data Ethics Oversight Group (for high-risk projects)
3. External Scrutiny -set up an external scrutiny mechanism (Independent Data Ethics Scrutiny Group) to provide external review and advice on data-driven/technology projects.
4. Accelerate development of internal Digital & Data Design Authority
5. Alignment to change process -embed guidance in Data Ethics Governance Framework into policing system Change Governance Processes
6. Maximise transparency -proactive, clear, comprehensive and accessible communications.
7. Consideration of future extension of the MoU principles and the approach of the data ethics framework and independent ethics group into broader areas across policing policy and practice to provide expert advice and assurance on human rights and ethical issues.

Finally, commentary on the workstream 4 report provided by Dr Brigit Schippers suggests that ethical decision making (including via the proposed sixth case) with respect to the deployment of emerging technologies in policing should consider several issues. Firstly, the identification and explication of ethics principles, e.g. beneficence and non-maleficence (‘do

no harm'); fairness, accountability, sustainability and transparency; and data protection principles for law enforcement. Secondly, the integration of ethics principles with relevant legal frameworks, for example through a combined 'ethics and law' case, including compliance with domestic and international legal frameworks of human rights, equality and data protection). Dr Schippers analysis also emphasised the importance of being clear about how Independent Ethics Advisory Panel members will be appointed and terms of reference agreed, the diversity of expertise and experience, what administrative and financial support there will be and how independence will be ensured. With regards to ethics triage consideration should also be given to protocols for recording ethics deliberations and decision-making, and the development of technology specific ethics case studies.

Chapter 8 summary and conclusions:

In justifying decisions and making them explainable, policing bodies are subject to oversight, with a focus on the public interest, by the Scottish Police Authority, and a number of other bodies, including for example His Majesty's Inspectorate of Constabulary Scotland, Audit Scotland, and the Information Commissioner's Office.

There has been a great deal of progress since 2019 to establish robust processes and mechanisms to underpin decision making and Police Scotland and the SPA have published a Memorandum of Understanding that outlines the principles through which decision making and engagement will be conducted. The MoU's stated focus on testing ethical, privacy and human rights issues; an engagement and communications plan to work with key stakeholders, the public and staff; full and transparent discussion; and informed decision making is certainly a positive development. There is also welcome mention of use of best available evidence, consideration of testing prior to full implementation, evaluation, and a baseline and post-implementation review process to evaluate the impact delivered and any organisational learning. Much of this will help underpin several key principles of accountable policing.

The 'four lines of defense' is a core component of SPA's Excellence Framework and the programme and project lifecycle process which a proposal would follow (as it develops from initial concept, through approvals to delivery) was outlined in detail above, and various potential enhancements are outlined below in several key considerations. As Lennon and Fyfe (2022) emphasise, *independence* is a key principle for accountability, and Lennon highlights the importance of consultation as a requirement, and SPA and other scrutiny bodies having sufficient resources to obtain independent input (particularly from technical advisors on technological assessments). Furthermore, as Chair I note that accountability principles such as *transparency* would be enhanced by routine collection and publication of data on police use of emerging technologies and their impacts, which will facilitate evaluation and ongoing scrutiny and review.

Police Scotland's proposed new Data Ethics Framework provides a methodology and mechanism to ensure that the goals of the MoU in relation to data ethics are implemented in a consistent and repeatable way, and indeed can be used to cover a wider consideration of equality and human rights issues. This would introduce a sixth ethics and human rights case. The framework is to be welcomed in that it aims to establish clear, robust governance

arrangements before investment (including external challenge and advice), clear responsibility and accountability putting repeatable processes in place to address and test ethical considerations and ensure consistency and auditability. However, as Raab (2020) acknowledges ethical frameworks can be complex, with norms and values that can be difficult to comprehend, and the real work is in their application. Therefore, it will be important to continually review and enhance the various new and developing ethics frameworks as they are embedded in policing in Scotland.

Key considerations relating to oversight, scrutiny and review are outlined briefly here (see Appendix C for more information):

8.1 The SPA and Police Scotland (PS) should **continue to use and enhance the arrangements set out in the MoU** to ensure future implementation of technology has the widest possible early engagement, consideration and external oversight.

8.2 SPA Board and Committees (and other bodies with decision making, oversight scrutiny and review functions) **should consider enhancing the informed nature of their consideration of proposals by inviting external subject matter experts** to provide evidence or advice on the impact technology may have on society.

8.3 The SPA (and other bodies) should **continue to require assurance that external evidence and advice has been sought and considered and that engagement with partners and the public has been undertaken to inform the approach to *embedding*** specific technologies in policing.

8.4 Policing bodies should consider the **routine collection, publication and accessibility of data on police use of emerging technologies and their impacts,** certainly for high-risk projects, in order to facilitate ongoing scrutiny and review.

8.5 The SPA and PS should continue to **develop a wider framework which sets out a systematic process for all ethical considerations, this should serve to guide the creation of a sixth ethics and human rights case which would be included in Initial and Full Business Cases.**

8.6 The Scottish Government should take the **learning from the *'Draft Proposals for Oversight of Ethical Considerations in Policing'* and consider endorsing a similar approach to enhancement of the Scottish Public Finance Manual** as good practice across all public bodies in Scotland.

8.7 **Policing bodies should implement the Data Ethics Framework across the policing system and an effectiveness review should be undertaken 12 months after the roll-out** to ascertain benefits realised and lessons learned.

8.8 **Policing bodies and scrutiny bodies must ensure that procurement processes used for new technologies** are compliant with all statutory requirements and best practice (including data protection, human rights and equalities impacts)**.**

8.9 **Scrutiny bodies should ensure PS continues to enhance its approach to ensuring effective and ongoing risk management processes** and continually **re-assesses and evaluates risks throughout the lifecycle** of any new technology.

8.10 **Policing bodies' complaints processes** (re police use of technology) **must be accessible to all members of the public including those with disabilities**. Where an **adverse human rights impact** to a person is the direct result of implementation of a new technology, those responsible for its implementation should provide an **effective remedy** (e.g. apology, compensation, restitution or cessation).

9. Conclusion and recommendations

Conclusion

Reflecting on the remit and terms of reference of the IAG, emerging technologies have an important role to play in supporting policing bodies to work collaboratively with partners to fulfil their statutory duties and the purpose of policing enshrined in the Police and Fire Reform Scotland Act (2012). Various technologies can play a key role in the investigation and detection of crime and efforts to prevent crime and harm and improve wellbeing and safety. For example, Ariel et al. (2015) found a link between BWV and reduced police use of force against citizens. However, technologies may not achieve their intended aims and indeed may have unintended consequences, for example, Koper et al. (2015) found that police use of mobile technology in hot spot policing was not effective in reducing crime, and rather was primarily used for surveillance and enforcement rather than strategic problem-solving. Whilst the potential for emerging technologies to assist with the detection and prevention of crime should be considered, a range of potential social and ethical implications (Connon et al., 2023) must also be explored. This highlights the value of a range of approaches: horizon scanning; drawing on the existing evidence base (from research and lessons learned from policing in other jurisdictions); and of conducting pilots and research evaluations of technological adoption in policing.

In relation to compliance with equality and human rights and data protection obligations our review suggests that EQHRIAs, DPIAs and other impact assessments are standard practice for policing bodies in Scotland, highlighting that improvements have been made over the last few years and learning has been taken on board since the issues with Cyber Kiosks. For example, proactive consultation and the formulation of operational guidance occurred in the buildup to the introduction of Body Worn Video in armed policing in late 2021. Nonetheless, although the legal basis specified in DPIAs appears to be more likely to be shared with key stakeholders for input now, given the potential for differing interpretation it would be good practice to share the legal basis (and opinions being drawn on) with a variety of external stakeholders as a matter of course in order that they may be questioned, tested and reviewed.

Further to policing legislation, key domestic and international legislation and relevant case law relating to emerging technologies in policing including Human Rights, Equalities, Data Protection, Biometrics and Law of Evidence were reviewed and found to form a decent basis for Police Scotland to exercise their powers. However, global research and best practice in relation to legislative and ethical frameworks suggests that legal frameworks or binding codes of practice (as opposed to guidelines) provide more clarity and are preferable when dealing with certain applications of technology in policing, e.g. automated decision making and AI (particularly in predictive policing) and live facial recognition, given the legal, social and ethical issues identified. In relation to the regulation of biometric data by the police however, Scotland is set to become a forerunner as a result of the Scottish Biometrics Commission's Code of Practice.

With regards to ethical frameworks, Police Scotland has Ethics Advisory Panels in place, though suggestions have been made to enhance independence and transparency. A significant positive development will be the planned introduction of the new Data Ethics Framework and associated proposed sixth ethics and human rights case, which will likely be of interest to other police forces. Oversight by SPA and partners has been substantially enhanced in recent years, together with the signing of the Memorandum of Understanding between Police Scotland and SPA. This represents a positive step, for example the focus on external challenge and advice fits with the importance of consultation and independent input as a key accountability principle.

Beyond the key areas above outlined in the terms of reference, i.e. legal and ethical frameworks and oversight, the IAG's review emphasises some other crucial areas: the centrality of research evidence and evaluation, consultation and public engagement, innovation and tests of change, and the importance of scientific standards. Furthermore, we highlight the importance of training, partnerships, ongoing knowledge exchange and how crucial the routine collection, publication and accessibility of data is to ongoing review and evaluation, particularly in relation to the equality and human rights impacts of police use of emerging technologies.

In conclusion, significant steps have been taken by policing bodies in Scotland to bring improvements to the approach taken in adopting emerging technologies in policing. The recommendations below will serve to position Scotland as world leading in adopting a rights based, ethical, evidence-based, consultative and robust approach to innovation and adoption of emerging technologies in policing. The key will be ensuring that innovation and technological adoption is *fostered* in order to enable police to fulfil their statutory duties and enhance public safety. Therefore, the level of scrutiny and evaluation required should vary depending on the existing evidence base and level of risk.

We hope that the associated learning and developments relating to the introduction of emerging technologies in policing in Scotland will be useful to other areas of policing, and will be of interest internationally. It is our ambition that the work of the group will support the embedding of technology in policing in a manner that upholds public confidence and supports efficient and effective policing that is rights based, transparent, ethical and socially responsible and delivers, rather than erodes, social justice.

Recommendations

Theme 1: Business case development, implementation and processes

1. Policing bodies (Police Scotland and SPA Forensic Services) should continue to adhere to the guidance set out in the HM Treasury Green book for the Strategic Case. This includes ensuring an **assessment of the current available evidence base** (including benefits and dis-benefits) across jurisdictions and other police and public services and relevant published research is included in the Case for Change section within the Business Case. (for more details see Appendix C, key consideration 3.1)

2. The **assessment of the Ethical and Human Rights Impact** of emerging technologies should be evidenced and a proportionate judgement for the implementation or

otherwise of technology should be included in Business Cases. This could take the form of a 6th Ethical and Human Rights Case, which would be a first for the UK and should make full use of EQHRIA, DPIA, CRWIA, Community and Islands Impact Assessments, Fairer Scotland Duty Impact Assessment, independent expert advice, Ethics Advisory Panels (EAPs), other relevant impact assessments and the results from the new Data Ethics Governance Framework within Police Scotland. The 6th case should draw a proportionate judgement using all of the evidence, research and advice available on if and how the technology should be adopted by policing. The SPA and PS should continue to develop the creation of a framework of guidance on the development of a 6th case. This is in addition to Police Scotland ensuring that all new technology introduced is compliant with the Equality Act 2010 and associated Codes of Practice and meets the requirements of the Equality Act 2010 (Specific Duties) (Scotland) Regulations 2012, including the duty to assess and review policies and practices.

3. Policing bodies introducing emerging technologies, applied in a context which impacts how the public are policed, should publish a clear and **publicly accessible Operational Practice Code**, ensuring compliance with relevant statutes or codes of practice. This document should be developed with external input and set out the conditions and limitations of use of the technology, safeguards in place and the methods by which compliant application for a policing purpose is maintained and overseen.

4. Police Scotland should seek to implement, as soon as possible, their **Data Ethics Governance Framework**. Key stakeholders (e.g. DPO) should be involved in internal review and scrutiny prior to implementation and an effectiveness review should be undertaken 12 months after the roll-out to ascertain the benefits realised and lessons learned during implementation.

5. Project implementation and lifetime management should ensure appropriate **training** for officers who will be utilising or monitoring emerging technology (particularly AI enabled technologies), with a particular focus on equality, human rights and data protection obligations.

6. When developing future proposals for technology use, policing bodies should consider, where appropriate, utilising small **tests of change/pilots** which could be externally evaluated to inform Business Cases and shape wider scale implementation within the Policing System. A system or process should be developed to ensure a standardised approach to this and should include using service design principles and data protection by design and default from development through to implementation.

7. When adopting emerging technology policing bodies should ensure **standards** are designed to meet the needs of users and enable interoperability within and between public agencies and compliance with data protection, equalities and human rights law. More broadly adherence to ISO, scientific and other relevant standards and codes (such as the ICO Data Sharing Code and Children's Code) should be designed at the outset of any new technology implementation. Policing bodies could consider establishing a national technology clearing house to ensure robust scientific standards for AI technologies. Internal standards, policies and procedures around the development and use of AI should that draw on the ICO's AI and Data Protection Guidance. An Algorithmic impact assessment policy

should be considered and algorithms should be published via the UK's Algorithmic Transparency Standard.

8. Police Scotland should continue to enhance its approach to ensuring effective and mature **risk management** processes by scoping, mapping, identifying and addressing any risk (particularly risks to rights and freedoms of individuals), opportunity or issue which may become associated with the adoption of a new technology and continuing to re-assess and evaluate risks throughout the lifecycle of any new technology. This includes the requirement to regularly review, update and implement data protection and equality impact assessments.

Theme 2: Transparency, engagement and evaluation

9. Police Scotland should continue to develop and implement the **Consultation and Engagement Framework** described in this report when considering the adoption of emerging technology. Engagement should align with legal and governance frameworks, occur as early as possible, have clarity of purpose, draw on the evidence base, be inclusive and accessible (including vulnerable groups and those who may have greatest risk of adverse impacts), include an element of formal consultation, enable colleague voice, promote ongoing dialogue, provide clear public facing communication, be transparent about how insights will be and are used and consider involving the public and stakeholders in formulating guidelines (see Appendix C key considerations 3.2, 6.1-6.12). Summaries of EAP meetings should be made public to aid transparency.

10. Police Scotland should clearly specify the **legal basis** for using emerging technology, share it with key stakeholders for input and publicly share it.

11. As part of the lifetime management of a new technology/project, policing bodies should have a clear **evaluation plan** which seeks to gather data (including baseline measurements) so that the emerging risks and efficacy can be assessed and DPIAs reviewed and updated throughout the lifecycle. The decision about whether a research evaluation is needed should be taken early on and informed by the level of risk and existing evidence base. A communication plan should seek to inform and regularly update scrutiny bodies and the public on operational usage and the delivery of the intended public benefit (or any dis-benefits) of the technology.

Theme 3: Legislation and policy

12. Whilst significant legislative gaps were not found, Scottish Government (and where appropriate SBC) should seek to keep the legislative landscape under review and consider whether future technological deployments would benefit from the introduction of **statutory codes of practice** in order to provide greater clarity and safeguards on the application of emerging technologies in policing (such as Live Facial Recognition and certain applications of AI, e.g. in predictive policing). In future if there were plans to consider the deployment of autonomous security robotic devices in policing for enforcement purposes new legislation should be introduced in advance. However, the possibility that certain applications of some technologies in policing should be categorically prohibited from use, either because they are unacceptably risky even with mitigation in place, or because they are intrinsically incompatible with human rights, should be considered in this context by Government.

13. The Scottish Government should take the learning from the *'Draft Proposals for Oversight of Ethical Considerations in Policing'* and consider endorsing a similar approach to enhancement of the Scottish Public Finance Manual as good practice across all public bodies in Scotland.

14. Policing bodies' (Police Scotland, SPA and PIRC) **complaints processes** must be clearly communicated prior to the start of new technology initiatives in policing and be accessible to all members of the public including those with disabilities. Where an adverse human rights impact to a person is the direct result of implementation of a new technology, those responsible for its implementation should provide an **effective remedy**.

15. Policing bodies should, at an early stage, ensure that **data flows** and the roles and responsibilities of all relevant parties under data protection law are mapped and understood. This is critical to ensuring that data can flow as intended, in compliance with data protection law and that the introduction of technology and subsequent collection of data does not result in increased victimisation, inequalities and inefficiencies or unjustly adversely impact on individuals' rights and freedoms. Where data sharing takes place, appropriate data sharing agreements should be in place and the ICO's Statutory Data Sharing Code of Practice should be complied with.

Theme 4: Oversight

16. The SPA (and other oversight bodies) should continue to require assurance that **external evidence, research and advice** has been sought and considered in the development of cases and that engagement with partners and the public has been undertaken to inform the approach to embedding specific technologies in policing. This should include evidence of early engagement in accordance with the Joint MoU and the use of subject matter experts to advise and inform scrutiny bodies' oversight of emerging technology initiatives.

17. The SPA (and other oversight bodies) should continue to implement a system to **regularly review** (and consider how Independent EAPs might feed in) the assessment of the public benefit, any risks, harms, positive or negative impacts of the introduction and use of emerging technology projects.

18. Policing and scrutiny bodies should consider the routine **collection, publication and accessibility of data** on the equality and human rights impacts of police use of emerging technologies, at least for high-risk projects, in order to facilitate ongoing scrutiny and review.

References

Akhgar, B., Bayerl, P.S., Bailey, K., Dennis, R., Gibson, H., Heyes, S., Lyle, A., Raven, A. and Sampson, F. (2022) Accountability Principles for Artificial Intelligence (AP4AI) in the Internal Security Domain. AP4AI Framework Blueprint.

Alikhademi, K., Drobina, E., Prioleau, D. et al. (2022), A review of predictive policing from the perspective of fairness. Artificial Intelligence Law, 30, 1–17, https://doi.org/10.1007/s10506-021-09286-4

Almeida, D., Shmarko, K., and Lomas, E. (2021). The ethics of facial recognition technologies, surveillance, and accountability in an age of artificial intelligence: a comparative analysis of US, EU, and UK regulatory frameworks. AI Ethics, https://doi.org/10.1007/s43681-021-00077-w

Ariel, B., Farrar, W.A. & Sutherland, A. (2015). The Effect of Police Body-Worn Cameras on Use of Force and Citizens' Complaints Against the Police: A Randomized Controlled Trial. J Quant Criminol 31, 509–535. https://doi.org/10.1007/s10940-014-9236-3

Asaro, P. (2019). AI Ethics in Predictive Policing: From Models of Threat to an Ethics of Care, IEEE Technology and Society Magazine, 38, 2, 40-53, June 2019, doi: 10.1109/MTS.2019.2915154

Aston, E., O'Neill, M., Hail, Y., and Wooff, A. (2021a) Information sharing in community policing in Europe: building public confidence. European Journal of Criminology. https://journals.sagepub.com/doi/full/10.1177/14773708211037902

Aston, E., Murray, K., & O'Neill, M. (2021b). Achieving cultural change through organizational justice: The case of stop and search in Scotland. *Criminology & Criminal Justice*, *21*(1), 40–56. https://doi.org/10.1177/1748895819839751

Aston, E., Wells, H., Bradford, B. and O'Neill, M. (2022), Technology and Police Legitimacy in Verhage, A. et al. (eds.) Policing and Technology in Smart Societies. Switzerland: Palgrave. Pp. 43-68.

Babuta, A., (2017), Big Data and Policing: An Assessment of Law Enforcement Requirements, Expectations and Priorities. Royal United Services Institute for Defence and Security Studies.

Babuta, A., and Oswald, M., (2020) Data Analytics and Algorithms in Policing in England and Wales: Towards A New Policy Framework, Royal United Services Institute for Defence and Security Studies.

Bloch, S. (2021). Aversive racism and community-instigated policing: The spatial politics of Nextdoor. Environment and Planning C: Politics and Space. https://doi.org/10.1177/23996544211019754

Binns, R. (2022) Human Judgment in algorithmic loops: Individual justice and automated decision-making, Regulation & Governance, 16, 197-211, doi:10.1111/rego.12358.

Birchley, G, Huxtable, R., Murtagh, M. et al. (2017), Smart homes, private homes? An empirical study of technology researchers' perceptions of ethical issues in developing smart-home health technologies. BMC Med Ethics 18, 23, https://doi.org/10.1186/s12910-017-0183-z

Bradford, B., Yesberg, J. A., Jackson, J., and Dawson, P., (2020). Live Facial Recognition: Trust and Legitimacy as Predictors of Public Support For Police Use of New Technology, The British Journal of Criminology, 60, 6, 1502–1522, https://doi.org/10.1093/bjc/azaa032

Bragias, A., Hine, K., & Fleet, R., (2021) 'Only in our best interest, right?' Public perceptions of police use of facial recognition technology, Police Practice and Research, 22, 6, 1637-1654, DOI: 10.1080/15614263.2021.1942873

Brewster, B., Gibson, H., and Gunning, M. (2018). Policing the Community Together: The Impact of Technology on Citizen Engagement. Societal Implications of Community Oriented Policing Technology. 91--102. https://doi.org/10.1007/978--3--319--89297--9_11

Brookman, F., & Jones, H. (2022) Capturing killers: the construction of CCTV evidence during homicide investigations, Policing and Society, 32, 2, 125-144, DOI: 10.1080/10439463.2021.1879075

Buchanan, B. et al. (2023) Research evidence, technological innovation and scientific standards in policing workstream report of the IAG. - https://www.gov.scot/ISBN/978-1-80525-350-1

Bullock, K. (2018). The Police Use of Social Media: Transformation or Normalisation? Social Policy and Society, 17, 2, 245-258. doi:10.1017/S1474746417000112

Campbell, K. et al. (2023) Informed decision-making, community engagement and participation workstream report of the IAG. - https://www.gov.scot/ISBN/978-1-80525-348-8

Clavell, G. (2018), Exploring the ethical, organisational and technological challenges of crime mapping: a critical approach to urban safety technologies. Ethics Inf Technol 20, 265–277. https://doi.org/10.1007/s10676-018-9477-1

Chowdhury, M. (2020) Nonparametric models for longitudinal data: With implementation in R, Wu, Colin O., Tian, Xin, Boca Raton, FL: CRC Press - https://doi.org/10.1111/biom.13223

Connon, I.L.C., Egan, M., Hamilton-Smith, N., Mackay, N., Miranda, D., & Webster, C.W.R. (2023) Review of emerging technologies in policing: Findings and recommendations to the IAG. - https://www.gov.scot/ISBN/978-1-80525-351-8

Daly, A. et al. (2023) Legal frameworks and ethical standards workstream report of the IAG. - https://www.gov.scot/ISBN/978-1-80525-347-1

Dechesne, F. (2019). AI & Ethics at the Police: Towards Responsible use of Artificial Intelligence in the Dutch Police. Leiden/ Delft: Universiteit Leiden.

Depeau, J. (2018) Graph technology is in the pole position to help law enforcement - Graph Technology Is in the POLE Position to Help Law Enforcement [Video] (neo4j.com)

Egbert, S., & Krasmann, S. (2020) Predictive policing: not yet, but soon preemptive?, Policing and Society, 30, 8, 905-919, DOI: 10.1080/10439463.2019.1611821

Ellis, J., (2019) Renegotiating police legitimacy through amateur video and social media: lessons from the police excessive force at the 2013 Sydney Gay and Lesbian Mardi Gras parade, Current Issues in Criminal Justice, 31. 3, 412-432, DOI: 10.1080/10345329.2019.1640171

Ellison, M., Bannister, J., Lee, W. D., & Haleem, M. S. (2021). Understanding policing demand and deployment through the lens of the city and with the application of big data. Urban Studies, 58, 15, 3157–3175. https://doi.org/10.1177/0042098020981007

Ernst, S., ter Veen, H., and Kop, N. (2021). Technological innovation in a police organization: Lessons learned from the National Police of the Netherlands, Policing: A Journal of Policy and Practice, 15, 3: 1818–1831, https://doi.org/10.1093/police/paab003

Facca, D., Smith, M. J, Shelley, J., Lizotte, D., and Donelle, L. (2020), Exploring the ethical issues in research using digital data collection strategies with minors: A scoping review. PLoS ONE 15(8): e0237875. https://doi.org/10.1371/journal.pone.0237875

Fukada-Parr, S., & Gibbons, E. (2021) Emerging consensus on 'Ethical AI': Human rights critique of stakeholder guidelines - https://doi.org/10.1111/1758-5899.12965

Fung, A. (2006) Varieties of participation in complex governance - https://doi.org/10.1111/j.1540-6210.2006.00667.x

Goldsmith, A. (2015) Disgracebook policing: social media and the rise of police indiscretion, Policing and Society, 25, 3, 249-267, DOI: 10.1080/10439463.2013.864653

Furuhaug, R.A., "Open source intelligence methodology," Master's thesis, School of Computer Science and Informatics, University College Dublin, 2019.

Fussey, P., & Sandhu, A. (2020). Surveillance arbitration in the era of digital policing. Theoretical Criminology. https://doi.org/10.1177/1362480620967020

Hamilton-Smith, N., McBride, M., & Atkinson, C. (2021) Lights, camera, provocation? Exploring experiences of surveillance in the policing of Scottish football, Policing and Society, 31, 2, 179-194, DOI: 10.1080/10439463.2019.1696800

Hayward, K. J., & Maas, M. M. (2021). Artificial intelligence and crime: A primer for criminologists. Crime, Media, Culture, 17, 2, 209–233. https://doi.org/10.1177/1741659020917434

Hendl, T., Chung, R. & Wild, V. (2020), Pandemic Surveillance and Racialized Subpopulations: Mitigating Vulnerabilities in COVID-19 Apps. Bioethical Inquiry 17, 829–834. https://doi.org/10.1007/s11673-020-10034-7

Hendrix, J. A., Taniguchi, T., Strom, K. J., Aagaard, B. & Johnson, N. (2019) Strategic policing philosophy and the acquisition of technology: findings from a nationally representative survey of law enforcement, Policing and Society, 29, 6, 727-743, DOI: 10.1080/10439463.2017.1322966

Henne, K., Shore, K., & Harb, J. I. (2021). Body-worn cameras, police violence and the politics of evidence: A case of ontological gerrymandering. Critical Social Policy. https://doi.org/10.1177/02610183211033923

Hobson, Z., Yesberg, J.A., Bradford, B. et al. (2021), Artificial fairness? Trust in algorithmic police decision-making. J Exp Criminol. https://doi.org/10.1007/s11292-021-09484-9

Hood, J., (2020), Making the Body Electric: The Politics of Body-Worn Cameras and Facial Recognition in the United States, Surveillance and Society, 18, 2, 157-169

Holley, C., Mutongwizo, T., Shearing C., (2020), Conceptualizing Policing and Security: New Harmscapes, the Arithropocene, and Technology, Annual Review of Criminology, 3, 341-358, DOI10.1116/annurev-criminol-011419-041330

Joh, E. (2019). Policing the smart city. International Journal of Law in Context, 15, 2, 177-182. doi:10.1017/S1744552319000107

Joyce, N. M., Ramsey, C. H., & Stewart, J. K. (2013). Commentary on Smart Policing. Police Quarterly, 16, 3, 358–368. https://doi.org/10.1177/1098611113497043

Keenan, B. (2021), Automatic Facial Recognition and the Intensification of Police Surveillance. The Modern Law Review, 84: 886-897. https://doi.org/10.1111/1468-2230.12623

Klauser, F. (2021). Policing with the drone: Towards an aerial geopolitics of security. Security Dialogue. https://doi.org/10.1177/0967010621992661

Kleinig, J. (1996), The ethics of policing - https://doi.org/10.1017/CBO9781139172851

Kjellgren, R. (2022). Good Tech, Bad Tech: Policing Sex Trafficking with Big Data. International Journal for Crime, Justice and Social Democracy, 11,1, 149-166. https://doi.org/10.5204/ijcjsd.2139

Koper, C. S., Lum, C., & Hibdon, J. (2015). The uses and impacts of mobile computing technology in hot spots policing. Evaluation Review, 39,6, 587–624.

Laufs, J., & Borrion, H. (2021). Technological innovation in policing and crime prevention: Practitioner perspectives from London. International Journal of Police Science & Management, 24, 2: 190–209. https://doi.org/10.1177/14613557211064053

Lennon, G & Fyfe, N 'Principles for accountable policing' (Police foundation, 2022) - Principle of Accountable policing.pdf (scottishinsight.ac.uk)

Leslie, D. (2019). Understanding artificial intelligence ethics and safety: A guide for the responsible design and implementation of AI systems in the public sector. The Alan Turing Institute. https://doi.org/10.5281/zenodo.3240529

Lindeman, D. A., Kim, K. K., Gladstone, C., and Apesoa-Varano, E. C., (2020), Technology and Caregiving: Emerging Interventions and Directions for Research, The Gerontologist, 60, 1: S41–S49, https://doi.org/10.1093/geront/gnz178

Lum, C., Stoltz, M., Koper, C. S., & Scherer, J. A., (2019). Research on body-worn cameras: What we know, what we need to know. Criminology & Public Policy 18: 93– 118. https://doi.org/10.1111/1745-9133.12412

Lumsden , K., & Black, A. (2020) 'Sorry, I'm dead, it's too late now': barriers faced by D/deaf citizens when accessing police services, Disability & Society, DOI: 10.1080/09687599.2020.1829555

Lynch, N., Campbell, L., Purshouse, J. and Betkier, M. (2020), Facial Recognition Technology in New Zealand: Towards a Legal and Ethical Framework, The Law Foundation of New Zealand.

Lynch, N. and Chen, A. (2021), Facial Recognition Technology: Considerations for use in Policing. An independent report commissioned by New Zealand Police.

Malgieri, G., and Niklas, J., (2020), Vulnerable data subjects, Computer Law & Security Review, 37, 105415, https://doi.org/10.1016/j.clsr.2020.105415

McGuire, M. R. (2021) The laughing policebot: automation and the end of policing, Policing and Society, 31, 1, 20-36, DOI: 10.1080/10439463.2020.1810249

McKendrick, K. (2019) Artificial Intelligence Prediction and Counterterrorism - https://apo.org.au/node/261706

M. MacNeil, M. Koch, A. Kuspinar, D. Juzwishin, P. Lehoux, and P. Stolee, "Enabling health technology innovation in canada: barriers and facilitators in policy and regulatory processes," *Health Policy*, vol. 123, no. 2, pp. 203– 214, 2019.

M. C. Matusiak and W. R. King, "Advancing the study of police innovation: Toward an empirical definition and classification of contemporary police innovations," *Crime & Delinquency*, vol. 67, no. 12, pp. 1982–2010, 2021.

Meijer, A., & Thaens, M. (2013) Social media strategies: Understanding the differences between North American police departments, Government Information Quarterly, 30, 4, 343-350, https://doi.org/10.1016/j.giq.2013.05.023

Miliaikeala, S. J. Heen, J., Lieberman, D., & Miethe, T. D. (2018) The thin blue line meets the big blue sky: perceptions of police legitimacy and public attitudes towards aerial drones, Criminal Justice Studies, 31, 1, 18-37, DOI: 10.1080/1478601X.2017.1404463

Milner, M. N., Rice, S., Winter, S. R., & Anania, E. C. (2020) The effect of political affiliation on support for police drone monitoring in the United States. Journal of Unmanned Vehicle Systems, 7, 2, 129-144. https://doi.org/10.1139/juvs-2018-0026

Miranda, D. (2022) Body-worn cameras 'on the move': exploring the contextual, technical and ethical challenges in policing practice, Policing and Society, 32, 1, 18-34, DOI: 10.1080/10439463.2021.1879074

Murphy, J. R., & Estcourt, D. (2020) Surveillance and the state: body-worn cameras, privacy and democratic policing, Current Issues in Criminal Justice, 32, 3, 368-378, DOI: 10.1080/10345329.2020.1813383

Neiva, L., Granja, R., & Machado, H. (2022) Big Data applied to criminal investigations: expectations of professionals of police cooperation in the European Union, Policing and Society, DOI: 10.1080/10439463.2022.2029433

Nellis, M. (2014), Upgrading electronic monitoring, downgrading probation: Reconfiguring 'offender management' in England and Wales, European Journal of Probation, 6, 2, 169-191, DOI: 10.1177/2066220314540572

Neyroud, P., & Disley, E. (2008), Technology and Policing: Implications for Fairness and Legitimacy, Policing: A Journal of Policy and Practice, 2, 2, 226–232.

Noriega, M., (2020) The application of artificial intelligence in police interrogations: An analysis addressing the proposed effect AI has on racial and gender bias, cooperation, and false confessions, Futures, 117, 102510, https://doi.org/10.1016/j.futures.2019.102510.

O'Connor, C. D. (2017) The police on Twitter: image management, community building, and implications for policing in Canada, Policing and Society, 27, 8, 899-912, DOI: 10.1080/10439463.2015.1120731

Oswald, M., & Babuta, A. Machine Learning Predictive Algorithms and the Policing of Future Crimes: Governance and Oversight (2019) - https://ssrn.com/abstract=3479081

Oswald, M. (2022), 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, European Journal of Law and Technology, 13, 1: https://ejlt.org/index.php/ejlt/article/view/883/1045

Page, A., & Jones, C. (2021) Weaponizing neutrality: the entanglement of policing, affect, and surveillance technologies, Feminist Media Studies, DOI: 10.1080/14680777.2021.1939400

Raab, C. (2020) Information privacy, impact assessment, and the place of ethics, *Computer Law & Security Review*, Volume 37, https://doi.org/10.1016/j.clsr.2020.105404

Ronquillo, C.E., Peltonen, L.-M., Pruinelli, L., Chu, C.H., Bakken, S., Beduschi, A., Cato, K., Hardiker, N., Junger, A., Michalowski, M., Nyrup, R., Rahimi, S., Reed, D.N., Salakoski, T., Salanterä, S., Walton, N., Weber, P., Wiegand, T. and Topaz, M. (2021), Artificial intelligence in nursing: Priorities and opportunities from an international invitational think-tank of the Nursing and Artificial Intelligence Leadership Collaborative. J Adv Nurs, 77: 3707-3717. https://doi.org/10.1111/jan.14855

Ross, S., (2023) Oversight, scrutiny and review workstream report of the IAG.- https://www.gov.scot/ISBN/978-1-80525-349-5

Sakiyama, M., Miethe, T., Lieberman, J. et al. (2017), Big hover or big brother? Public attitudes about drone usage in domestic policing activities. Security Journal, 30, 1027–1044. https://doi.org/10.1057/sj.2016.3

Sanders, C. B. & Henderson, S. (2013) Police 'empires' and information technologies: uncovering material and organisational barriers to information sharing in Canadian police services, Policing and Society, 23, 2, 243-260, DOI: 10.1080/10439463.2012.703196

Schwarz J, Bärkås A, Blease C, Collins L, Hägglund M, Markham S, and Hochwarter S. (2021), Sharing Clinical Notes and Electronic Health Records With People Affected by Mental Health Conditions: Scoping Review JMIR Mental Health 8 (12): e34170

Shore, A., K. Prena, and J. J. Cummings, "To share or not to share: Extending protection motivation theory to understand data sharing with the police," *Computers in Human Behavior*, vol. 130, p. 107188, 2022.

Smith, M., & Miller, S. (2022), The ethical application of biometric facial recognition technology. AI & Soc 37, 167–175 https://doi.org/10.1007/s00146-021-01199-9

Strom, K., and Smith, E. L., (2017), The Future of Crime Data: The Case for the National Incident-Based Reporting System (NIBRS) as a Primary Data Source for Policy Evaluation and Crime Analysis, American Society of Criminology, 16, 4: 1027-1048. DOI:10.1111/1745-9133.12336

Cass R. Sunstein, Irreversible and Catastrophic (John M. Olin Program in Law and Economics Working Paper No. 242, 2005).

Todak, N., Gaub, J. E. and White, M. D. (2018), The importance of external stakeholders for police body-worn camera diffusion, Policing: An International Journal, 41, 4, 448-464. https://doi.org/10.1108/PIJPSM-08-2017-0091

Ulucanlar, S., Faulkner, A., Peirce, S., and Elwyn, G. (2013), Technology identity: The role of sociotechnical representations in the adoption of medical devices, Social Science & Medicine, 98: 95-105. https://doi.org/10.1016/j.socscimed.2013.09.008.

Urquhart, L., & Miranda, D. (2021) Policing faces: the present and future of intelligent facial surveillance, Information & Communications Technology Law, DOI: 10.1080/13600834.2021.1994220

Van Eijk, C. (2018). Helping Dutch Neighborhood Watch Schemes to Survive the Rainy Season: Studying Mutual Perceptions on Citizens' and Professionals' Engagement in the Co-Production of Community Safety. Voluntas 29, 1: 222--236. https://doi.org/10.1007/s11266-017--9918--1

W. E. Bijker, Of bicycles, bakelites, and bulbs: Toward a theory of sociotechnical change. MIT press, 1997.

Walsh, J. P., & O'Connor, C. (2019). Social media and policing: A review of recent research. Sociology Compass, 13, e12648. https://doi.org/10.1111/soc4.12648

Whittlestone, J. Nyrup, R. Alexandrova, A. Dihal, K. Cave, S. (2019) Ethical and societal implications of algorithms, data, and artificial intelligence: a roadmap for research. London: Nuffield Foundation

Williams, D. P. (2020), Fitting the description: historical and sociotechnical elements of facial recognition and anti-black surveillance. Journal of Responsible Innovation, 7, supplement 1, 74-83. DOI: 10.1080/23299460.2020.1831365

Williams, M., Butler, M., Jurek-Loughrey, A., & Sezer, S. (2021) Offensive communications: exploring the challenges involved in policing social media, Contemporary Social Science, 16, 2, 227-240, DOI: 10.1080/21582041.2018.1563305

Williams, M. L., Edwards, A., Housley, W., Burnap, P., Rana, O., Avis, N., Morgan, J., & Sloan, L. (2013) Policing cyber-neighbourhoods: tension monitoring and social media networks, Policing and Society, 23, 4, 461-481, DOI: 10.1080/10439463.2013.780225

Završnik A. Algorithmic justice: Algorithms and big data in criminal justice settings. European Journal of Criminology. 2021;18(5):623-642. doi:10.1177/1477370819876762

Zhu, J., Shi, K., Yang, C., Niu, Y., Zeng, Y., Zhang, N., Liu, T., & Chu, C. H. (2021). Ethical issues of smart home-based elderly care: A scoping review. Journal of Nursing Management, 1– 14. https://doi.org/10.1111/jonm.13521

Appendix A

IAG meetings

The Independent Advisory Group met on the following dates:

- 15 December 2020
- 11 March 2021
- 26 May 2021
- 26 August 2021
- 17 November 2021
- 24 February 2022
- 26 April 2022
- 31 May 2022
- 24 August 2022
- 27 October 2022

In addition, the workstreams met individually over a number of dates throughout the review period.

Membership of workstreams Appendix B

WS1 legal frameworks and ethical standards

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

WS2 evidence and scientific standards

- Professor Bill Buchanan, Edinburgh Napier University (Chair)
- Georgie Henley, techUK
- Sam Curran, Scottish Police Authority
- Stephen Roberts, Home Office Accelerated Capability Environment
- Dr Matthias Wienroth, Northumbria University
- Superintendent Stevie Dolan, Police Scotland
- Dr Megan O'Neill, University of Dundee and SIPR
- Basil Manoussos, Edinburgh Napier University

WS3 consultation and community engagement

- Kirsty-Louise Campbell, Head of Strategy and Insight Police Scotland (Chair)
- Davina Fereday, Senior Manager: Research and Insight, Police Scotland
- Kevin Ditcham, Insight and Engagement Lead, Police Scotland
- Colin Lee, Race Equality, CEMVO Scotland
- Annie Cook, Network & Delivery Manager, Democratic Society
- Eve Georgieva, Senior Service Designer, Scottish Government
- CS Matt Richards, SRO, BWV Programme, Police Scotland
- Dave Shea, Senior National Development Officer, Scottish Community Safety Network
- Dr Nick Bland, Visiting Professor, Edinburgh Napier University
- Dr Andrew Wooff, Associate Professor, Edinburgh Napier University
- David Allan, Deputy Director, Scottish Community Development Centre

WS4 oversight, scrutiny and review

- Scott Ross, Scottish Police Authority (Chair)
- Elaine Galbraith, His Majesty's Inspectorate of Constabulary in Scotland
- Naomi McAuliffe, Amnesty International
- Diego Quiroz, Scottish Human Rights Commission
- Dr Genevieve Lennon, University of Strathclyde
- Denis Hamill, Police Scotland Chief Data Officer
- Sam Curran, Scottish Police Authority

Key considerations Appendix C

Ch3 research evidence key considerations

3.1 **All business cases** (and hence templates) **completed by policing bodies should require the inclusion of a basic assessment of the evidence base, drawing on available research (and learning from other jurisdictions) and including both benefits and dis-benefits.** The level of risk (see chapter 8) should determine the level of evidence gathering required. For medium-risk projects (or projects with high value investment) an evidence review should be required. For all high-risk projects a more thorough evidence review (ideally with external input or review) should be required, or indeed in some cases the generation of further independent research may be necessary (particularly if the evidence base is lacking) to inform decision making regarding adoption. [covered in Recommendation 1]

3.2 Policing bodies should also **draw together the evidence base to support consultation and public engagement work**. A balanced, clear and succinct public facing summary of the existing research and other evidence (acknowledging any limitations and gaps in knowledge) should be developed (with input from independent external stakeholders, particularly for high-risk projects) in order to be shared during public engagement and consultation exercises. [R 9]

3.3 **The decision about whether an evaluation of the impact of new technologies in policing is needed should be informed by the level of risk and the existing evidence base.** For existing systems with a history of safe operation an evaluation would only be necessary if they undergo significant changes in their design or intended purpose. For high-risk projects an evaluation should be carried out and commenced at the earliest point possible prior to development, acquisition or adoption of a new tool, means or method of policing. Third party support (e.g. through SIPR) with commissioning research should be sought very early on and the evaluation should include baseline impact measurements. Steps should be taken to safeguard the quality and independence of the evaluation e.g. establishing a Research Advisory Group and peer reviewing of reports. [R 11]

3.4 In addition to accessing learning and research on best practice in the use of emerging technologies from other jurisdictions (including from other police forces) to inform decision making (e.g. business cases and sixth case assessment) and design processes, **opportunities for knowledge exchange (where possible in open fora) should continue to be maximised by policing bodies throughout implementation and ongoing review.** [learning point]

3.5 The existing knowledge base and **suggestions for further research identified by Connon et al. (2023) should be reviewed by policing bodies and key stakeholders in order to prioritise areas for further research**. An assessment should be undertaken of the level strategic importance, level of risk, and potential value of the research in order to guide decision making on which areas should be prioritised for funding by various partners (Scottish Government, Police Scotland, Scottish Police Authority, the Scottish Institute for Policing Research etc.). In addition, suggestions should be shared with SIPR and wider the

academic community who are keen to undertake independent research and leverage external funding e.g. from research councils. [learning point]

Ch 4 Legal Frameworks key considerations

4.1 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; and 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 suggest that 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. [R 2, R 5]

4.2 **Further consideration of impacts of 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 (e.g. through sixth ethics -case see ch8) 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 key consideration we seek to aid compliance and raise 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 individuals' 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 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. [R 2]

4.3 **Legal basis for using policing powers vis-à-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. [R 10]

4.4. Whilst significant legislative gaps were not found, Scottish Government (and where appropriate SBC) should seek to keep the legislative landscape under review and consider whether future technological deployments would benefit from the introduction of **statutory codes of practice** in order to provide greater clarity and safeguards on the application of emerging technologies in policing (such as Live Facial Recognition and certain applications of AI, e.g. in predictive policing). In future if there were plans to consider the deployment of autonomous security robotic devices in policing for enforcement purposes new legislation should be introduced in advance. However, the possibility that certain applications of some technologies in policing should be categorically prohibited from use, either because they are unacceptably risky even with mitigation in place, or because they are intrinsically incompatible with human rights, should be considered in this context by Government. [R 12]

4.5 **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 suggest that Police Scotland conduct, embed and enhance Child Rights and Wellbeing Impact Assessments (CRWIAs) alongside DPIAs and EqHRIAs. [R 2]

4.6 The use of new technologies should not unlawfully or 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. Positive impacts should also be considered and taken into account. The legal requirement to carry out an Equality Impact Assessment for any revised policy or practice includes the requirement (legislation.gov website link) to consider evidence relating to or received from people with protected characteristics. [R 2]

4.7 Police Scotland should **seek to publish Operational Practice Codes** as soon as reasonably possible prior to the implementation of technology. Police Scotland should seek to produce **proactive communications** on the use and effectiveness of specific technology post implementation, this should be a concerted effort to ensure as wide an audience as possible. 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 considered by Police Scotland given the likelihood drones will capture sensitive personal data and have a high risk of collateral intrusion. [R 11, learning point]

4.8 Attention should be paid to the personal data generated by technologies used by policing bodies. It is critical that mission creep is managed. Data must be processed for a specific, explicit and legitimate purpose and in line with the data minimisation and data limitation principle. Any onward data sharing must be in line with the ICOs Data Sharing Code of Practice and DPIAs and Data Sharing Agreements should be in place. Regular reviews should be carried out. Additional safeguards should apply where processing relates to children and vulnerable people as the risks of harm is likely to be higher. All new systems must be capable of compliance with data protection law. [R 15]

4.9 New technologies often involve complex data flows with multiple partners. It is critical that before implementation due diligence is carried out so that data flows are mapped and understood and the **roles and the obligations of all partners under data protection law are understood**. Particular attention needs to be paid in the context of competent authorities commissioning private vendors to process personal data to develop and train algorithmic systems. Any data sharing must be compliant with data protection law and policing bodies should be particularly careful that personal data processed for law enforcement purposes is not shared with non- law enforcement partners unless it is authorised by law. [R 15]

Ch 5 Ethical and social implications & best practice considerations

5.1 **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. [learning point]

5.2 **The SPA and PS should continue to use, embed and continually improve the processes set out in relation to Ethics Advisory Panels (EAPs).** For example, Regional and National EAPs should invite external subject matter experts. Police Scotland should publish anonymised minutes of EAPs (or at least a summary of meeting discussions and outcomes) in order to enhance transparency. A clear explanation of how the findings and advice of EAPs helped shape the solution, planned implementation or preferred option for a new technology should be required in a new section of the Full Business Case template. Police Scotland should consider how the EAPs can be involved in a system of rolling review, from proposal/pilot to implementation, in order to track progress of technology projects and to give ongoing advice. Police Scotland's EAP framework, including Terms of Reference and relationship with legal compliance should be reviewed in order to ensure the framework is being appropriately operationalised, sufficiently transparent, independent and appropriately resourced. Note an independent data ethics group is being set up. [R 9, 17]

5.3 Consideration could be taken of a number of potential policy and practice recommendations are highlighted by Connon et al. (2023: 134-139), relating to various technologies (electronic database technologies, biometric identification systems and AI technologies, surveillance systems and tracking devices) which will be of interest and may be found in full on pages 4-7 and 142-143 of the Stirling report. [learning points]

5.4 a) Policing bodies and scrutiny bodies should ensure a monitoring mechanism **to record data on its equality and human rights impacts,** is incorporated into the design and implementation of an emerging technology. Ethnicity data should be collected and reported transparently in order to help protect minority groups. In order to demonstrate due regard to the 3 needs general equality duty, Police Scotland should routinely gather and use equality information relevant to all protected characteristics. Policing bodies should make data on the equality impacts of trial use of technologies publicly available. [R 18]
b) **Training** should be given (linked to Codes of Practice and Standard Operating Procedures) to all officers involved in the use or monitoring of emerging technologies to ensure they are aware of their equality and human rights obligations in the context of its use. Force polices, guidance, and training (developed in accordance with EA2010 and PSED) may be used to inform officers and staff about ethical standards and the methods in which behaviour is compliant with bias mitigating efforts. [R 5]

Ch 6 Consultation and public engagement key considerations

[all Ch 6 considerations incorporated into recommendation 9]
6.1Policing bodies should **ensure engagement and consultation considerations align effectively with both legal and governance frameworks, and consideration of ethics** via an appropriate organisational model.

6.2 Policing bodies should be **clear on the purpose of the engagement process from the outset** – what people are going to influence, why and how.

6.3 Policing bodies should **engage at an early stage in the governance process to understand views and sub-groups where a greater understanding of concerns is needed.** Using focus groups and other methods can give an early overview of key areas for consideration. This is critical for complex or less understood technology (such as AI and predictive analytics) and high-risk projects.

6.4 Policing bodies should include an **element of formal consultation in the approach to ensure that the views of the public and communities are both appropriately considered and embedded at an appropriate point** e.g. in decision making, a pilot or prior to the roll out of all new and emerging technology. A formal consultation process has the safeguard of judicial review processes where the public and communities are able to challenge.

6.5 Policing bodies should set out to have an **ongoing dialogue with the public utilising participatory approaches where appropriate**, as the technology is considered and during/ after implementation. This will enable concerns, risks, and suggestions for improvement to be considered and addressed at all stages of the governance process.

6.6 Policing bodies should use a **clear and transparent engagement framework underpinned by engagement principles and quality assurance to ensure the process, explanation of risk and benefit and ethical and human rights considerations are clear and well-articulated**. This will guide the design of engagement which can be tailored, in terms of levels of participation and methods, to meet the individual considerations of the technology and potential impacts.

6.7 Policing bodies should ensure **all engagement and consultation processes are inclusive and accessible for everyone, including protected groups defined in the**

Equality Act 2010 and ensure representation from a variety of Scotland's communities. This should occur at as early a stage as possible.

6.8 Policing bodies should enable the **colleague voice to be heard as a key element of shaping proposals.** For effective service delivery, an open two-way dialogue that is safe and inclusive, and facilitates a reciprocal exchange of ideas and feedback should identify any problems or conflicts, and solutions to improve the quality of police-citizen interactions, as technology is introduced and embedded (with appropriate training, communications, Code of Practice, assurance and transparency). This can contribute to ensuring transparency and justifying proportionality.

6.9 Policing bodies should ensure **engagement insights, providing a clear narrative of the views of the public and communities, are considered and scrutinised by governance bodies**. This must include areas of concern and how these are being balanced, addressed and mitigated.

6.10 Policing bodies should make a **public, open and transparent commitment to *how* the insights from the engagement process will be used to shape the consideration and implementation of new technology and also report back with details, which are made publicly available and scrutinised**. As part of this, details should be included on the manner in which the use of new and emerging technology will be monitored post implementation. Clear routes should be provided for the public to provide feedback, raise concerns or suggest improvements. How these have been addressed should be visible for scrutiny bodies and reported in an open and transparent manner.

6.11 Policing bodies must **communicate with the public and other stakeholders about police technology capabilities and substantial changes to the dynamic of police work mediated by technology**. **This communication must be clear, public 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.

6.12 Policing bodies should **involve key stakeholders and members of the public in the formulation of police guidelines in the use of technologies** (such as surveillance systems and tracking devices e.g. BWV) to involve them and provide understanding of the rules. This should reduce controversy regarding their implementation with the public and stakeholders.

Ch7 Technological Innovation and Scientific Standards considerations

7.1 Technology innovation is not just about getting the technology right, but about socio-technical change, which includes cultural change in practice, institutions, and oversight. In order to facilitate successful adoption into practice, **policing bodies should prepare an implementation plan which assesses and takes into consideration stakeholder perceptions, existing systems and practices at practitioner, policy and oversight levels** and a variety of other elements that may be impacted on and are likely to have to innovate at the same time. [learning point]

7.2 Technology innovation is a longer-term process, including at the implementation level. In relation to decisions about procurement, replacing systems or changes to practice,

policing bodies should focus on **establishing understanding and the willingness to experiment** e.g. in small-scale test-runs. [R 6]

7.3 Partnerships are important for technological innovation and can strengthen the capacity for socio-technical change, encourage benefits to arise from such change and render innovation more socially acceptable. Organisations in the policing system and their partners should **invest in developing stable, longer-term mutual collaboration between industry, academia and public organisations**. [learning point]

7.4 Policing bodies should **adopt next generation standards designed to meet the needs of the user and enable interoperability** within and between forces to reduce cost, risk and complexity and conform to published specifications for storage, sharing and security and ensure a common understanding of what good looks like. For example, policing bodies should put a stronger focus on inter-agency approaches to secure data sharing, including the adoption of POLE and MAIT. More broadly policing bodies should integrate with developing standards from outside policing and should consider suggestions (Buchanan et al., 2023: 28-29). [R 7]

7.5 Policing bodies should consider **establishing a national technology clearing house to ensure robust scientific standards for AI technologies.** [R 7]

Ch 8 Oversight, Scrutiny and Review key considerations

8.1 **The SPA and Police Scotland (PS) should continue to use and enhance the arrangements set out in the MoU** to ensure any future implementation of technology has had the widest possible appropriate and early engagement and consideration and external oversight. [Recommendation 16]

8.2 **SPA Board and Committees** (and other bodies with decision making, oversight scrutiny and review functions) **should consider enhancing the informed nature of their consideration of proposals by inviting external subject matter experts or representatives** from professional reference or ethics panels to provide evidence or advice on the impact that a specific technology may, or is, having on society. [R 16]

8.3 The SPA (and other bodies) should **continue to require assurance that external evidence and advice has been sought and considered and that engagement with partners and the public has been undertaken to inform the approach to *embedding*** specific technologies in policing. [R 16]

8.4 Policing bodies should consider the **routine collection, publication and accessibility of data on police use of emerging technologies and their impacts,** certainly for high-risk projects, in order to facilitate ongoing scrutiny and review. This should be made available to oversight bodies, for research purposes (certainly where there is a limited evidence base) and where possible made accessible to the public in order to provide transparency, promote public confidence, support learning and knowledge exchange and demonstrate effective oversight. More information should be published and made accessible publicly, for example Police Scotland should regularly publish data on biometrics they hold, e.g. how many Scottish images are in CHS and PND in the same way that SPA publish data on DNA and fingerprints. The minutes of relevant bodies e.g. Biometrics

Oversight Board should also be published in a manner that enhances accessibility of the information. [R 18]

8.5 **The SPA and PS should continue to develop a wider framework which sets out a systematic process for all ethical considerations, this should serve to guide the creation of a sixth ethics and human rights case which would be included in Initial and Full Business Cases.** The framework should inform decision making through consideration of data ethics and wider consideration of equality, privacy and human rights issues. (Appendix 3 Ross et al. 2023). [R 2]

8.6 The Scottish Government should take the **learning from the *'Draft Proposals for Oversight of Ethical Considerations in Policing'* and consider endorsing a similar approach to enhancement of the Scottish Public Finance Manual** (which incorporates the Green Book) **as good practice across all public bodies** [R 13]

8.7 Policing bodies should **implement the Data Ethics Framework** (and its key aspects) **across the policing system and an effectiveness review should be undertaken 12 months after the roll-out** to ascertain the benefits realised and lessons learned during implementation. [R 4]

8.8 **Policing bodies and scrutiny bodies must ensure that procurement processes used for new technologies** are compliant with all statutory requirements and best practice including a focus on data protection, human rights and qualities impacts**.** For example, the HM Treasury Green Book's business case framework will be enhanced by the inclusion of a sixth ethics and human rights case. Whilst Police Scotland work on the principle of 'Re-use, before Buy, Before Build', in house development may be preferable in some situations, in which case robust design guidance such as data protection by design should be followed and a system of independent quality checking would be desirable. [learning point]

8.9 Police Scotland should **continue to enhance its approach to ensuring effective and ongoing risk management processes** by scoping, mapping, identifying and mitigating any risk, opportunity or issue which may become associated with the adoption of a new technology, and continuing to **re-assess and evaluate risks throughout the lifecycle of any new technology**. With this risk based approach greater emphasis should be placed on considering future impacts of technology and ways to understand how communities may respond to proposals. Scrutiny bodies ensuring that policing bodies continually evaluate risks throughout the lifecycle of the technology will also allow them to ensure risks which become evident after deployment are acted on. [R 8]

8.10 **Policing bodies' complaints processes regarding police use of technology must be accessible to all members of the public including those with disabilities**. Where an **adverse human rights impact** to a person is the direct result of implementation of a new technology, those responsible for its implementation should provide an **effective remedy**. An effective remedy may include an apology, provisions to ensure the harm cannot recur, compensation (financial or other) for the harm, restitution or cessation of a particular activity or some other form of remedy agreed by the parties. [R 14]

Scottish Government
Riaghaltas na h-Alba

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: 978-1-80525-352-5 (web only)

Published by The Scottish Government, February 2023

Produced for The Scottish Government by APS Group Scotland, 21 Tennant Street, Edinburgh EH6 5NA
PPDAS1212302 (02/23)

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