# Review of emerging technologies in policing

Connon, Irena Leisbet Ceridwen; Egan, Mo; Hamilton-Smith, Niall; MacKay, Niamh; Miranda, Diana; Webster, C. William R.

*Publication date:*
2023

# Review of emerging technologies in policing: findings and recommendations

February 2023

Scottish Government
Riaghaltas na h-Alba

**Emerging technologies in policing**

# Review of emerging technologies in policing: Findings and recommendations

**Final report**

**July 2022**

Authors:

Irena L. C. Connon

Mo Egan

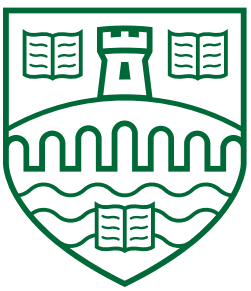
Niall Hamilton-Smith

Niamh MacKay

Diana Miranda

C. William R. Webster

UNIVERSITY of STIRLING



**Contents**

## Executive Summary

### Introduction

This report has been compiled for the Scottish Government's "Emerging Technologies in Policing" project, and was commissioned by the Scottish Institute for Policing Research (SIPR) acting on behalf of the Scottish Government. It is based on a review of emerging technologies in policing undertaken between January and July 2022. The review was completed by a research team based at the University of Stirling.

The review considered: 1) the social and ethical implications of particular types of emerging technologies in policing practice, 2) the legal considerations associated with the adoption of emerging technologies in policing, 3) recommendations from the existing research examining the trial and adoption of new emerging technologies in policing, as well as for ethical and scientific standards frameworks and guidelines, for informing best practice and wider dissemination of these technologies in police practice, 4) recommendations for the use of emerging technologies in policing based on experiences from other sectors (Health, Children and Family), and 5) the lessons learnt and recommendations that can be made from the analysis of existing case law concerning emerging technology. The report provides a descriptive overview of the relevant literature and case law available, as well as a series of recommendations for best practice in the implementation and dissemination of the different forms of technology in police practice

The types of emerging technologies in policing practice considered in this review are electronic databases, biometric identification systems and artificial intelligence (AI), and surveillance systems and tracking devices.

### Methodology

The review consisted of four components. These were:

1. A systematic search and review of interdisciplinary social science (published) academic research literature focusing on the development, trial, and implementation of emerging technologies in policing practice;
2. A review of relevant policy-relevant (grey) literature consisting of research reports, practice-based evidence reports and policy reports (published and unpublished) not available through the academic research literature databases;
3. A supplementary systematic search and review of academic literature focusing on the trial and implementation of forms of emerging technologies identified in component one within the literature focusing on the health care and children and families' sectors and
4. A legal search and legal case review to map the regulatory frameworks guiding the police use of emergent technology (equality and human rights, data protection and evidence).

## Findings and Discussion

### Social and Ethical Issues

The analysis revealed that there were various social and ethical issues associated with three different forms of emerging technologies: 1) electronic databases, 2) biometric identification systems, and 3) surveillance systems and tracking technologies.

#### 1) Electronic databases

Specific social and ethical implications were identified for in relation to the use of electronic databases. The technologies discussed in the literature differed, with most debate focused on data sharing, third-party data sharing platforms, social media, and vulnerable populations. A common issue highlighted in the literature related to how information is stored and accessed, particularly when managing sensitive information. Differences in organizational practice and the lack of alignment in organizational culture, resulted in barriers to data sharing processes, were also frequently raised in the literature reviewed. Further issues raised included the risk posed to privacy and human rights and the risk of enhancing social injustices. The latter was particularly manifest in community policing application data, with a focus on social exclusion and perpetuation of racial inequalities. This has an impact on public trust and legitimacy, issues also discussed in relation to social media application information. The literature focused on vulnerable populations databases and datasets also highlighted the opportunities and risks associated with surveillance of vulnerable groups and the need for more engagement and consultation with these groups.

The report concludes that far less is known about the particular social and ethical issues associated with open-source data, data pulling platforms and DNA databases than other types of electronic database technologies, with less empirical evidence available for these types of technologies.

#### 2) Biometric Identification Systems

Different biometric systems were discussed in the literature, in particular facial recognition, AI (Artificial Intelligence) smart sensors, emotional recognition, and voice pattern analysis tools. More is known about facial recognition technologies and artificial intelligence technologies compared to voice pattern recognition systems.

Issues of accuracy, fairness and transparency were particularly discussed in relation to AI. Public trust and legitimacy were important factors to consider, particularly in relation to the use of facial recognition. Issues related to privacy and personal security were also highlighted in relation to the deployment of these technologies. A common issue in these systems also related to the risk of enhancing inequalities for marginalized groups and the potential for racial and gender bias. Lastly, the lack of standards, ethical principles and guidance emphasized the need for ethical guidelines and laws for risk minimisation.

#### 3) Surveillance Systems and Tracking Devices

Different systems were presented in the documents reviewed: drones, smart devices and sensors, location and ‘Hot spot’ analysis, body worn cameras, autonomous

security robots, CCTV, and visual/optical technologies. The concerns relating to privacy were common when discussing the increased level of surveillance allowed by these systems, especially when targeting minority communities. The issue of legitimacy in relation to the use of these systems was also presented, particularly in relation to the deployment of drones and smart devices in policing practice. Issues with public confidence and trust were also highlighted. Public perception can impact technology deployment and there are certainly implications for police practice and for public-police relationships (this is particularly evident with body-worn cameras). Little is known about the social and ethical implications concerning the use of autonomous security robots compared to other forms of surveillance and tracking technologies.

When discussing the impacts associated to the use of these technologies, it is important to understand that due to their emergent nature, it is not yet possible to fully understand the ethical, social, and legal implications. Future consequences might be anticipated in order to identify risks and benefits of using specific technologies. However, it is important to note that the process of assessing the impacts and consequences of emerging technologies should be an ongoing process, owing to its emerging nature. This literature and legal framework review addresses the potential ethical, social, and legal issues associated with emerging technologies in policing.

## Legal Issues

The review found that the main legal issues associated with emerging technologies concern the law of evidence, especially in relation to improperly obtained evidence, disclosure of evidence, data protection, and human rights and equality. In particular, the use of emerging technologies is highly likely to challenge the boundaries of the Criminal Procedure (Sc) Act 1995, Regulation of Investigatory Powers (Scotland) Act 2000, Investigatory Powers Act 2016, as well as compliance with the National Assessment Framework for Biometric Data Outcomes and prospectively the Scottish Biometric Commissioners' Code of Conduct. Specific legal issues are associated with each of the different forms of emerging technology (namely in relation to data processes and data protection). Appendix 3 identifies UK case law relevant to the adoption of emerging technologies in policing. International case law is also considered in Appendix 4. Appendix 5 outlines the key legislative provisions associated to each technology, supported by relevant case law. A comparative view on good practice in the design of law, policy, and practice is drawn in particular from Canada and New Zealand.

## Recommendations for Research, Policy, and Practice

Although the amount of literature containing evidence-based recommendations from which to develop best practice in the rollout of emerging technologies in policing was more limited than the body of literature evidencing the social and ethical issues associated with these forms of technology, a range of recommendations were identified for the different types of technology. Sections 3.3 and 3.4 outline the lessons learnt from the existing research and recommendations for **good practice** for the implementation of emerging technologies in policing. These recommendations were drawn from the **literature** discussing the trialing and

adoption of these technologies in **policing** and as well as in **other sectors** (e.g., Health, and Children and Families).

## 1. Recommendations for Electronic Database Technologies

A total of thirteen recommendations were drawn from the review for improving best practice in the development and implementation of electronic database technologies. These recommendations include recommendations for policy and practice, as well as for enhanced collaboration between policy makers, practitioners and researchers in research processes and developments aimed at improving the use of these forms of technology in policing.

- **Recommendations for research:**

1. 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.
2. 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.
3. 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.

- **Recommendations for policy and legislation:**

1. For MASH (Multi-Agency Safeguarding Hubs) to be developed and implemented to allow for better data sharing practices with partner agencies. They should be underpinned by the development of a clear decision-making framework at the national level to ensure ethical storage, management, and use of data, as well to help safeguard the data on vulnerable individuals.
2. The need for standardized guidelines to be developed and implemented to ensure that technology does not result in increased victimisation, inequalities and inefficiency in its storage and use.
3. There needs to be a careful mapping of data flows to ensure that roles within the data protection framework can be established and legal obligations complied with.
4. Where consent is not the ground on which lawful processing is based, the processing must be necessary for the performance of a task carried out for law enforcement purposes, or if for sensitive data, there must be an appropriate policy document in place.
5. The Data Protection Act 2018 gives a very narrow definition of law enforcement purposes and so, where a database is being used for purposes beyond that scope, consideration needs to be given to the lawful basis of processing.
6. Specific guidelines for working with social media data should be developed.
7. Cross sectoral discussion (e.g. between Police and Health and Social Care) should be undertaken to co-develop guidelines or standards concerning the use of these technologies with minors or to hold data about minors to address concerns around uncertainty.

- **Recommendations for practice:**

1. For the standardisation of practice with professionals from other government sectors (e.g., health, social work) who may have different cultures and practices regarding the collection, storing, processing and use of data.
2. Guidance and training should be provided to better prepare professionals working in policing and in other sectors that work closely with members of the police (e.g., social workers who work with the police in custodial and probation contexts) on how to write notes and input data to ensure greater standardization of practice.
3. Specific guidelines should also be provided for police and closely affiliated professionals regarding subject access to records and data held about them. Appropriate scrutiny and oversight mechanisms should also be established.

**2. Recommendations for Biometric Identification Systems and Artificial Intelligence Technologies**

The following recommendations for research, policy, legislation, and practice were drawn from the literature concerning the development and use of biometric identification systems and artificial intelligence technologies in policing:

- **Recommendations for research:**

1. The need for further research to be conducted to explore the benefits and limitations of the use of facial recognition technologies in different policing activities (namely, public order policing, crowds, and public events).
2. 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.
3. 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.
4. The need to interrogate biases and limitations as to the efficiency of AI systems prior to development.
5. 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.

- **Recommendations for policy and legislation:**

1. The need to devise new ethical principles and guidelines for technology use, considering the need for support from the general public.
2. The need for the development and provision of guidelines or clear processes for the scrutiny, regulation, and enforcement of biometric identification systems, including facial recognition technologies, as part of a new draft code of practice which should specify the responsibilities for policing bodies regarding scrutiny, regulation, and enforcement of these new standards.
3. For mandatory equality impact assessments to be introduced, as well as for the collection and reporting of ethnicity data to help to protect minority groups.

4. Use of Oswald's (2019) three-pillar approach to develop a national ethical approach that includes clear scientific standards for these forms of technology.
5. Establishment of a national technology clearinghouse for ensuring robust scientific standards for AI technologies.
6. Development of an algorithmic impact assessment policy and make this compulsory prior to the use of the algorithm.
7. Development of specific policy for the trial and adoption of new technologies before deployment.

- **Recommendations for practice:**

1. The adoption of an Ethics of Care approach (based on the work of Asaro (2019) to minimise the risk of harm in the dissemination and use of these technologies and to improve perceptions of fairness regarding Artificial Intelligence technologies.
2. For templates to be developed to implement the algorithmic impact assessment.
3. Staff should be trained in how to engage critically with the adoption and use of new technologies (particularly AI enabled technologies) so that they are in a position to meaningfully engage in impact assessments.

**3. Recommendations for Surveillance Systems and Tracking Devices**
The following recommendations can also be made for the implementation, use and dissemination of these forms of technologies in policing:

- **Recommendations for research:**

1. For trials to be conducted 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.

- **Recommendations for policy and legislation:**

1. For key stakeholders and members of the public to be involved in the formulation of police guidelines concerning the use of these technologies, especially to democratise the rules around body-worn cameras and reduce controversy regarding their implementation with public and third-party stakeholders.
2. For very strict ethical codes and laws to be implemented for the use of autonomous security robotic devices in policing.
3. For clear standards and principles to be developed concerning the use of these technologies in forensic investigations.

- **Recommendations for practice:**

1. For greater training to be provided and for greater emphasis to be given to the behavioural effects that these forms of technology may have on officers.

**4. Data protection, the law of evidence, and equality and human rights: Recommendations applicable to all forms of emerging technologies**

In addition, the following recommendations are applicable to all the above forms of emerging technologies and targeted towards ensuring compliance with the law of evidence, data protection, and equality and human rights:

- **Recommendations for research:**

1. 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.
2. The relationship between those involved in the development and implementation of emerging technologies should be mapped for data protection purposes. There is also a need to understand the nature of the data being processed and the scope of that processing (see ICO report box).
3. 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.

- **Recommendation for policy:**

1. An equality and human rights impact assessment should form a compulsory part of the trial and adoption of any new technology policy. This should facilitate consideration of these issues on a cyclical process before adoption, during deployment, and after deployment. These impact assessments need to go beyond the minimum legal requirement of data protection and should consider the full range of impacts and consequences, including social and ethical impacts

- **Recommendations for practice:**

1. A monitoring mechanism should be incorporated into the design and implementation of an emerging technology to record data on its equality and human rights impacts.
2. Training should be given 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.
3. Data on the equality impacts of trial use of technologies should be made publicly available.

**A table summarising the recommendations (Table 4) is available on pages 142-143.**

## 1. Introduction

This report presents the findings from a study that focused on examining the social and ethical implications of emerging technologies for informing policing practice, and the legal considerations that need to be taken into account for the adoption of emerging technologies within the Scottish policing context. The study consisted of a systematic review of the social science research and policy-relevant literature, and a review of relevant case law, legislation, and appropriate legal literature. The study was commissioned by the Scottish Institute for Policing Research for the Independent Advisory Group on Emerging Technologies in Policing. The information presented in this report covers Key Focus Areas as part of the specified requirements for Workstreams 1 and 2, and as such, aims to identify best practice internationally in legislative frameworks surrounding emerging technologies, as well as ethical standards and legislative gaps (workstream 1), and international best practice in the use of research evidence for the development, adoption and implementation of ethical and scientific standards for emerging technologies in policing (workstream 2). This includes: examining good practice from other jurisdictions and fields, including comparing legal frameworks and ethical standards (WS1 KFA 2); considering the impacts of the adoption of emerging technologies on individuals' rights, the extent to which the existing legislation provides sufficient safeguards against these risks (WS1 KFA 5), whether there are any legislative gaps that need to be filled, and whether aspects of legal frameworks in other jurisdictions could fill any gaps (WS2 KFA 5); and how research may inform policy and practice concerning the development and use of scientific standards and ethical guidelines concerning emerging technologies (WS2).

To fulfil these requirements, this report provides a descriptive overview of the relevant literature and case law available, as well as recommendations for best practice in the implementation and dissemination of these forms of technology in police practice, including for the development and use of ethical and scientific standards frameworks. In addition, it highlights areas where further research and/or trials are required to be able to understand the implications of certain types of emerging technologies before new or additional recommendations can be made for mitigating any foreseeable negative impacts prior to implementation and/or wider dissemination in policing. Lists of areas where the application of current legislation remains untested and requires further consideration will also be identified for future exploration.

### 1.1: Emerging Technologies

The term ‘emerging technologies’ has gained traction in recent years in different public service and policy environments. Use of the term is quite fluid, but it is generally used to refer to a range of technologies, usually digital technologies, and in a number of different contextual settings. In the context of policing, many of these emerging technologies facilitate new information flows in and around the institutions of policing, and in doing so impact on internal structures and citizen-police interactions. Examples of emerging technologies in policing would include Electronic Databases, Automatic Face Recognition (AFR), Body-Worn Video (BWV) Cameras, Artificial Intelligence (AI), and Drones.

## 1.2: Defining Emerging Technologies

The term emerging technologies is generally used to describe a new technology, but it may also refer to the evolution of an existing technology or a planned implementation of a recently developed technology. It can also have different meanings when used in different areas, such as media, business, science, or public services. The term commonly refers to technologies that are currently developing, or that are expected to be implemented in the next five to ten years, and is usually reserved for technologies that are creating, or are expected to create, significant social, institutional, or economic impacts (Bray 2017; Kendal 1997; Whittlestone 2019; Wright and Friedewald 2013). Emerging digital technologies are often perceived to offer new business and service opportunities whilst, at the same time, pose challenges to existing ways of doing things. These include social, ethical, and legal challenges, and for digital technologies, these often relate to data processes and data protection. For public services, such as those agencies involved in policing policy and practice, such data processes are likely to involve the personal data of citizens and will have a bearing on citizen-state relations. When thinking about what constitutes an emerging technology, there are four key features that need to be considered:

1. The nature of the technology
2. The technological components
3. Applicational elements
4. Point of emergence

### 1.2.1: The Nature of the Technology

Emerging technologies in contemporary discourse are usually assumed to be digital technologies that support new information flows embedded in new information and communication technologies (ICTs). In this respect, such technologies involve data, including personal data, and data flows. Whilst emerging technologies may be defined by their digital component, they do not have to be exclusively digital and can comprise of other elements, including physical features. Philosophically, any physical artefact can be considered a technology, from the humble pencil through to satellite weaponry.

### 1.2.2: The Technological Components of Emerging Technologies

Emerging technologies are usually a configuration of a range of technological artifacts and are not really a single technology. For example, a surveillance camera system would include a camera, a network, monitors, and recording and storage equipment. As such, an emerging technology is really an assemblage of different components. So, when we talk about an emergent technology, we are not necessarily talking about the individual components of the technology, but often their combined integration into a new ‘technology’ or application. The emergent technology may therefore derive from the convergence of a number of technological developments including computerisation, miniaturisation and/or enhanced technological capability/capacity.

### 1.2.3: Applicational Elements: The Emergent Aspect of Emerging Technologies

Given that emerging technologies are comprised of several different components, it is unsurprising to suggest that not all of the components are new, or emerging, and

many have been in existence for a number of years. The emergent element of these technologies is their combination into a new application or artefact, or their introduction into a new service area (Stahl et al., 2017). Looking beyond the technical artefact, emerging technologies can also be considered emergent in that they facilitate emerging new informational relationships and ways of working. So, it may not be the technology that is new, but its introduction into a new service area, and the impacts that the technology has in that service area (Kendal 1997). Alternatively, it may be the case that an emergent technology has existed for many years, but that a new application has become envisioned that had not previously been foreseen (ibid).

### 1.2.4: The Point of Emergence

Emerging technologies are often at a different point of emergence. Some may be envisioned, but not yet in existence, others may be in development or being trialled, whilst others are already at the point of implementation, yet are still considered to be emerging. It may be that an emerging technology has been around for years, but that it has only recently diffused into a specific service setting.

A simple analytical framework for emerging technologies is presented in **Appendix 1**, which provides further detail as to how an emerging technology can be defined and specifically draws out the key features of an emerging technology

### 1.3: Implications and Consequences of Emerging Technologies

By definition, the full impact and consequences associated with the use of emergent technologies is not known and the implications of their use are uncertain and ambiguous (Sollie 2007). There may be perceived benefits of their use that do not materialise, or unintended consequences that do. Moreover, sometimes the visions bestowed on technologies by their advocates, in terms of what they will deliver, does not emerge in practice.

### 1.4: Rationale for the Study of Emerging Technologies

A key problem with emerging technologies is how to deal with the potential associated ethical issues that may result from a technology that is not fully entrenched in society (Bray 2017). As Whittlestone (2019) notes, technological innovation is comprised of several stages: 1) research, 2) development, 3) production, 4) marketing, and 5) diffusion into society. A technology that has completed all these stages is sometimes called an entrenched technology. Entrenched technologies are those that are widely used in society and have familiar uses and known impacts on society (Whittlestone 2019). The consequences of emerging technologies however are still not largely understood. For these to become successful and entrenched technologies, further research and/or testing may be required to understand their impacts (ibid). This is also the case for technologies that may have been developed a while ago because, ‘although they are known by researchers, decision makers and end users’ may not yet be aware of the potential outcomes of these technologies (Kendall 1997; Whittlestone 2019). According to

Brey (2012) the foreseeable future' in relation to technological development and embedding can be equated to a time frame of 10-15 years. This means that the 'emerging' phase within technological development may take up to 15 years and thus, it may take up to 15 years before the particular consequences associated with this form of technology may be fully known to an extent that is fully justifiable in terms of its broader rollout (Stahl et al., 2017, Brey 2012).

Given the uncertainty around emerging technologies, we can only make speculations about future products or the uses and impacts of recently developed technologies. However, by exploring research concerning the impacts of trials and elementary applications of recent technological developments (within the 15-year timeframe suggested by Brey 2012), early interventions can be made to mitigate any potential problematic impacts that may be associated with a particular technology. This is especially important considering that once a technology becomes entrenched in society or within a particular institution, it is very hard to make fundamental changes to its overall design and embedding in society (Bray 2017; Asante et al., 2014; Liebert and Schmidt 2010). So, unlike with entrenched technologies, there is more space for manoeuvre in the social embedding of emerging technologies. Examining the existing research focusing on trials and elementary application of new types of technological developments within a particular sector can help us anticipate the possible future consequences of its implementation more broadly within the sector (i.e., in other geographic and governance contexts) or its application and implementation across different sectors (Whittlestone 2019).

It is important to note however that it not possible to make definite or even reliable predictions about the exact nature of the consequences that the application or implementation of a technology will have within or across different societal sectors or in different contexts with emerging technologies. That said, analyses of the existing research can help identify plausible and possible outcomes which can help identify possible risks and benefits. In turn, this can help with strategic decision making and allow steps to be taken during the rollout of these technologies to avoid undesirable effects.

### 1.5: Aims of this Report: Emerging Technologies in Policing Practice

This study examines the current social, ethical, and legal issues associated with emerging technologies in policing with a view to improving best practice in the use of particular technologies in policing. In doing so, it aims to meet the required specifications for workstreams 1 and 2 in terms of identifying: a) best practice internationally in legislative frameworks, as well as ethical standards and legislative gaps, and b) international best practice for the development, adoption and implementation of scientific standards and ethical guidelines. As such, it focuses on the ways and extent to which the existing interdisciplinary research literature and has identified the range of issues associated with particular types of emerging technologies and the extent to which these have been arisen and been addressed in the existing legal frameworks. This will help to enable the identification of existing shortcomings in research capturing the impacts of use of these technologies in police practice, and in the application of the law in governing the use of these technologies. It will also help identify the key pre-requisites for best practice in the

implementation of these technologies more widely within the sector, and in integrated activities between the police and other public and private sectorial bodies.

### 1.5.1: Understanding the Social and Ethical Implications associated with Emerging Technologies for Best Practice in Policing

When defining what constitutes best practice for the embedding and rollout of a particular technology, it is necessary to first establish what is considered a socially desirable and acceptable direction. An important part of this process is understanding the possible ethical and social impacts that a particular technology may give rise to (Grunwald 2011; Jacob et al. 2013). This is because only with a clear understanding of the associated social and ethical issues can these be anticipated, reflected upon, deliberated with relevant stakeholders, and be responded to. Understanding these issues, as well as the recommendations made from research examining trials, and the implementation within one or more particular policing (or other sectoral) contexts, should therefore help decision makers to identify which technologies are desirable for further rollout, which pathways should or should not be pursued, and anticipate what can be undertaken or implemented in advance (by both policy and practice) to mitigate any potential negative impacts. It will also help to identify particular areas where further research and trials may be required.

Within this study, we consider the term ‘ethical and societal implications’, to refer to ways that emerging technologies may impact upon members of society or widely held values. The term ‘values’ refers to attitudes, beliefs and commitments that are deeply held and, generally speaking, widely shared by members of a particular society or closely, socio-culturally related society (e.g. considered to be collectively

held by members of Western societies, European societies, Euro-American society, or Scottish society as opposed to a particular cultural group within a wider society such as, for example, by members of a particular political party within Scottish society). As such, ethical implications are related to what people feel to be right or wrong (Stahl 2012; Stahl et al., 2017).

Given that this study is intended to inform best practice for the embedding of emerging technologies within Scotland, the scope of the review of research focusing on emerging technologies has been restricted to the development, trials, application and/or implementation of particular technologies in Western societies. This is because the (relatively) close overlap in terms of ethical beliefs as well as social structure and governance regime mean that the findings and recommendations are likely to be more comparably relevant for informing policy and practice in Scotland than the findings and recommendations obtained from research focusing on the social and ethical implications from other parts of the world with different governance regimes and socio-cultural systems.

### 1.5.2: Legal Implications associated with Emerging Technologies: The Legal Framework

The adoption of emerging technologies in policing presents a number of legal considerations. There are four areas that have to be evaluated for all technologies deployed in policing: compliance with the law of evidence, data protection, equality and human rights, and environmental impacts. Since this report is focused on

technologies in the context of police-citizen interactions, the potential environmental impact of specific technologies is beyond the scope of this study.

| **Recommendation** |
| --- |
| Environmental impact of the development and use of emerging technology should be the subject of specific research and processes should be assessed against Police Scotland's Environmental Strategy 2021. |

In terms of identifying gaps in the legal framework it is important to acknowledge that Scotland has a mixed legal system. This means it combines aspects of common law and civil law. The impact is that while the boundaries of legislation can be established, the boundaries of the common law are more dependent on the articulation and interpretation of legal principles (Bargenda and Wilson-Stark 2018). There are some areas of law where it is difficult to meaningfully assess how the law will be applied without a specific example of a type of technology and the context in which it is being used (Marchant 2011; Moses 2013).

The nature of the type of technology and its intended purpose will dictate which legal framework is likely to attach.

### 1.6: Research Questions

Our research questions are focused on two overarching key objectives:

1. Identification of best practice in legislative frameworks and ethical standards, as well as any legislative gaps surrounding emerging technologies and their adoption in policing practice, and

2. Identification of research evidence and best practice for the adoption and implementation of emerging technologies in policing, including for the development and use of ethical guidelines and scientific standards.

To achieve these objectives, we devised an approach to the study that focused on answering five key research questions:

1. What are the social and ethical implications of particular types of emerging technologies in policing?
2. What are the legal considerations associated with the adoption of emerging technologies in policing?
3. What recommendations can be made from the existing research examining the use of new emerging technologies in policing for best practice (including in relation to scientific standards and ethical guidelines) for the wider adoption and dissemination of these technologies in police practice, as well as for mitigating the social, ethical, and legal issues that may have arisen from the implementation of technological developments in trials and/or existing (limited) police practice?
4. What recommendations can be learnt for informing best practice in policing for the dissemination of emerging technologies from trials and/or the implementation of similar types of emerging technologies, and the application of associated scientific standards and ethical guidelines in the Health Care and Children and Families sectors?
5. What lessons can be learnt and what recommendations can made from the analysis of existing legal and ethical frameworks concerning emerging

technology for the adoption and dissemination of different forms of these technologies in the Scottish policing context?

### 1.7: Structure of Report

This report has been divided into several sections. The following section presents an overview of the methodology used to conduct the systematic review of the social science research and policy-relevant literature, searches for relevant primary sources (case law and legislation) and connected legal literature. This is then followed by an in-depth description of the findings for each of the research questions. The final section of the report consists of a concluding discussion where recommendations for good practice pertaining to the embedding and dissemination of emerging technologies in policing are made, as well as for further research to address identified shortcomings in the existing research focusing on specific technologies and to test the suitability and applicability of suggestions for good practice with the policing community for mitigating any of the negative (or potentially negative) social and ethical issues identified. Areas where the application of legal frameworks are untested or ambiguous will also be identified for future consideration.

## 2. Methodology

The study methodology consisted of four components:

1. Systematic search and review of the interdisciplinary social science (published) academic research literature focusing on the development, trial, and implementation of emerging technologies in policing practice.
2. Review of the relevant policy-relevant (grey) literature consisting of research reports, practice-based evidence reports and policy reports (published and unpublished) not available through the academic research literature databases.
3. Supplementary systematic search and review of the academic research literature focusing on the trial and implementation of forms of emerging technologies identified in component 1 within the literature focusing on the health care and children and families' sectors.
4. Legal searches identifying primary sources (case law and legislation) and secondary sources (academic commentary).

Each of these components will be discussed in turn in the following sub-sections.

### 2.1: Component 1: Systematic Review of the Interdisciplinary Social Science Research Literature focusing on the Development, Trial, and Implementation of Emerging Technologies in Policing Practice.

The first component review of the literature combined systematic and narrative techniques to review the existing academic literature focusing on emerging technologies in policing practice. This allowed the literature search to be conducted

in a way that adhered to the key principles of systemic reviewing (Bryman 2012), while simultaneously allowing for subjective evaluation of the literature to determine relevance (Snilsveit et al., 2012) and to identify gaps where future research needs to be undertaken.

### 2.1.1: Systematic Literature Search

The systematic aspect of the review drew on Bryman's (2012) approach to conducting a systematic review in the social sciences and was used to conduct database searches of the published academic research literature. First, three academic databases from which to perform keyword searches were identified and which reflected the interdisciplinary nature of the research problem. The databases selected were Web of Science, Scopus, and JSTOR. Key words relevant to the research question were identified to enable keyword searches of the databases to be performed using multiple combinations of keywords.

The searches generated articles of potential relevance to the first research questions, with an initial total of 1052 articles of potential relevance being identified. Further reductions using the methodology outlined below resulted in 143 articles being subjected to detailed review.

1) First, a pre-determined inclusionary /exclusionary criterion was applied to the initial search result.

   This resulted in articles published prior to the year 2007 being removed from the sample on the basis that articles 15 years or older can be deemed to be dated given that the focus of this review is on emerging technologies. The

decision to include articles up to 15 years old was determined on the basis that it can take up to 15 years for emerging technologies to move from the development, trial, and elementary application stage (research stages) to wider dissemination, embedding and entrenchment (Brey 2012) and that it can take up to 15 years for the potential impacts associated with particular technologies to be fully understood. Additionally, articles that had not been peer-reviewed in scholarly academic journals and those published in languages other than English were also removed. This resulted in 779 abstracts being excluded, bringing the number selected for inclusion and evaluation down to 268.

2) Duplicates in the number of articles were then removed. This brought down the total number to 201.

3) The titles and abstracts of the 201 articles were then scanned for evaluation in terms of their relevance to the key research questions and objectives of the project in a process constituting the first stage of the analysis. Articles which did not specifically focus on emergent technologies per se were removed on the basis that their relevance could not readily ascertained. This brought the total number of articles selected for inclusion down to 146.

4) Finally, given that the information and findings from this study will be drawn upon to develop guidelines for best practice, abstracts where the full article could not be accessed through the University institution were also removed. This is so that only the articles which can readily be drawn upon during

subsequent parts of the project were included in the final sample. This brought the final total of the number of articles selected for inclusion down to 143.

### 2.1.2: Analysis and Coding of the Academic Research Articles

Analysis and coding of the 143 articles included in the final sample was undertaken using qualitative descriptive analysis of each of the abstracts listed in **Appendix 2 Part A** to identify and code for key themes (Sandelowski 2000). The (inductive) coding process enabled the social and ethical issues associated with each of the different types of emerging technologies explored in the sample literature to be readily identified, along with recommendations for policing practice and future research. In addition, this process also enabled different types of technologies to be categorised into broader classificatory groupings according to their form (electronic databases, biometric identification systems, and surveillance technologies and tracking systems), which was necessary for synthesising the specific recommendations and for undertaking the analysis of the legal literature from which further recommendations could subsequently be drawn.

## 2.2: Component 2: Review of the Policy-Relevant (grey) Literature

As component 2 consisted of a review of research reports, practice-based evidence reports and policy reports (published and unpublished) which were not available through the academic research literature databases, an abridged version of the Delphi Technique was deployed which involved consultation with members of the wider project team and Advisory Group to obtain access to relevant reports. The

Delphi Method is a research technique that involves seeking and drawing on the extensive knowledge, skills, and expertise of academic experts and/or practitioners working on the issue of relevance (Barrett and Heale 2020, Dalkey and Helmer 1963). Given that with policy-relevant literature, publication may not necessarily guarantee the same level of quality control as can be expected by the peer-review process for academic literature published in academic journals (Adams 2016), it was important to seek expert verification that reports obtained for review could be deemed to be of sufficient quality for inclusion. From this, a list of 50 additional sources was produced for inclusion for detailed consideration as to their relevance for the purposes of this study.

Relevance was determined by close reading of the executive summaries or forewords. Thirty of these were deemed relevant for inclusion and subsequent analysis and coding. A list of these sources is provided in **Appendix 2 Part B.**.

Analysis and coding of the 30 documents obtained through the Delphi Method was undertaken in the same way as for the academic research literature, by using qualitative descriptive analysis to identify and code for key social and ethical issues with emerging technologies and particular recommendations made.

The total number of documents comprising both the academic research and policy-relevant literatures selected for inclusion in the final sample was 173.

## 2.3: Component 3: Supplementary systematic review of the academic research literature focusing on forms of emerging technologies identified in components 1 and 2 within the literature focusing on the health care and children and families' sectors

In order to determine further recommendations, lessons learnt and examples of good practice in the trialling and adoption of the forms of emerging technologies identified during the systematic review of the literature that may be transferable for their adoption and dissemination within policing practice, a supplementary systematic review of the research literature focusing on the different forms of emerging technologies within the Health and Children and Families sectors was undertaken. For this, a systematic keyword search was performed in the same way as for Component 1. However, owing to time constraints and given that the main focus of this study was on policing practice, selection for further consideration to determine relevance was restricted to the top 30 sources listed according to 'Relevance' from the keyword search. Relevance was determined on the basis of scrutiny of the title and abstract. Articles deemed relevant were then coded according to technology type and recommendations/lessons learnt/examples of good practice. Twenty-four articles were selected for inclusion in the final pool of articles for this supplementary review. A list of the sources deemed relevant, and which were reviewed to obtain recommendations from is provided in **Appendix 2 Part C.**

## 2.4: Component 4: Legal Searches

Relevant case law and legislation were identified using Westlaw[1], HUDOC[2], and LexisLibrary[3]. Having identified key provisions within the relevant legislation, this was supplemented with the examination of case law that informs the interpretation and application of those legislative provisions. The legal searches reflect the law as at 28 April 2022.

| | |
|---|---|
| UK Case Law | Appendix 3 |
| International Case Law | Appendix 4 |
| Legislation | Appendix 5 |

This research process involved:

- Using keyword searches, questions, and themes in the legal database search engines,
- The browsing of legislation overviews and case summaries to determine relevance, and
- Exploring the legislation and case analysis documents, which list significant cases cited as well as secondary sources that reference the relevant legislation/case.

[1] Westlaw: https://uk.westlaw.com/
[2] Hudoc: HUDOC - European Court of Human Rights (coe.int)
[3] LexisLibrary: Lexis®Library: Homepage (lexisnexis.com)

- Focusing on the implications of new emerging technologies in policing through the lens of human rights, the following human rights were identified as presenting significant challenges:
    - Right to a fair trial
    - Right to respect for private and family life, home, and correspondence
    - Right to freedom of assembly and association
    - Right to freedom from discrimination

Given that the nature of the type of technology and its intended purpose will dictate which legal framework is likely to attach, the legal analysis was structured around the three areas of 1) the law of evidence, 2) data protection, and 3) equality and human rights, and their application to the three broad categories of emerging technologies identified in Component 1: electronic databases, biometric identification systems, and electronic surveillance and tracking systems.

## 3. Findings and Discussion

In this section, the findings of our study are discussed in relation to each of the five research questions posed in turn.

### 3.1: The Social and Ethical Implications of Different Types of Emerging Technologies in Policing

The types of emerging technologies that the literature discussed spanned across three broad categories of technology type. These are:

1. Electronic Databases (mentioned in 59 out of a total of 173 documents)
2. Biometric Identification Systems (55 out of 173 documents)
3. Electronic Surveillance and Tracking Devices (52 out of 173 documents)[4]

The social and ethical issues associated with each of the different, specific types of technology that fall within each category are detailed in the following sub-sections.

#### 3.1.1: Electronic Databases

According to Bray (2017), data can be regarded as encoded information about one or

more target phenomena' (such as objects, events, processes, or persons). Nowadays, data is digitally rather than analogically encoded. Data is socially and ethically important for three reasons: 1) The process of collecting and organising data requires making

[4] Note that 9 of the articles within the sample referred to emerging technologies more generally and as such did not specifically focus on any one of the three key types of technology (electronic databases, biometric identification systems, or surveillance systems and tracking devise.

assumptions about what is significant or useful, meaning that in practice no dataset is ever fully objective or neutral; 2) Digitally encoded data allows information to be stored, managed, duplicated, shared, manipulated, and transformed more efficiently than before; and 3) Analysis of electronic data enables the processing of large amounts of data to obtain novel insights that may otherwise be inaccessible (Whittlestone et al., 2019). Electronic database technologies represent one form of continually evolving technology that are used in contemporary police practice. Electronic databases store, organize, and process information in a way that makes it easy to perform searches and analyses.

Fifty-nine of the 173 documents reviewed from the final sample discussed the use and management of electronic databases within the context of the implementation and use of emergent technologies in policing practice. The following specific types of electronic database technologies and uses were discussed in the literature:

- Data sharing and third-party data sharing platforms, including for public-private organisation data sharing purposes (17 of 59 documents)
- Community policing application data (16 of 59 documents)
- Data pulling platforms (2 of 59 documents)
- Social media application information (14 of 59 documents)
- Use of open-source data (4 of 59 documents)
- Vulnerable population databases and datasets (9 of 59 documents)
- DNA databases (4 of 59 documents)

3.1.1.1: Data Sharing and Third-Party Data Sharing Platforms

Seventeen of the 59 articles and reports that discussed electronic databases specifically addressed data sharing and third-party data sharing platforms (Asaro 2019; Babuta 2017; Babuta and Oswald 2020; Clavell 2018; Custers 2012; Henman 2019; McKendrick 2019; Neiva et al., 2022; Neyroud and Disley 2008; Skogan and Hartnell 2008; Sanders and Henderson 2013; Holley et al., 2020; Weaver et al. 2021, National Analytics Solutions 2017; Vilender et al. 2021). The social and ethical issues identified and discussed by these 17 articles fall into five thematic areas:

- 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

**a) Safety of Information Held**

Eleven documents discuss the importance of the safety of information storage and access in relation to electronic databases (Aston et al., 2021; Clavell 2018; Custers 2012; Leslie 2019; Neiva et al., 2022; Sanders and Henderson 2013; Vilender et al. 2021; Neyroud and Disley 2008; Babuta 2017; McKendrick 2019; Weaver et al., 2021). For example, Clavell (2018), using the example of Geographic Information System data in urban policing, discusses how ensuring the safety of data and preventing data access breaches requires organisations to confront a series of challenges relating to the organizational structures that will be used to manage them and their technical capacities and expectations in order to prevent the risk of increased victimisation, inequalities, or inefficiency. Leslie (2019) explores the risk of

‘data poisoning’, which is a type of adversarial attack that involves malicious compromise of data at the point of collection and pre-processing, and which can result from instances where data collection and procurement involve unreliable or questionable sources, including social media data and third-party curation processes. Sanders and Henderson (2013) examine the use of data sharing via computer aided dispatch systems and record management systems in relation to violent crime in Canada and the risks posed by potential beaches of information security. Similarly, Neiva et al. (2022) examines Big Data and the interoperability of multiple datasets, for criminal investigation and discusses the risks of the sharing of Big Data in relation to the potential for enforcing genetic discrimination with DNA databases, as well for privacy and human rights. Aston et al., (2021) discuss the role of data protection and security in relation to building public confidence and facilitating information sharing with the police online, as well as in face-to-face interactions.

**b) Human Rights and Privacy**

Eight of the 15 documents reviewed discuss the social and ethical implications of electronic databases and third-party information sharing systems by referring to the risks posed to privacy and human rights and the considerations that need to be made to mitigate these risks (Asaro 2019; Neiva et al., 2022, Holley et al., 2020; Vilender et al., 2021; Baburta 2017; Neyroud and Disley 2008; McKendrick 2019; Sanders and Henderson 2013). For example, Holley et al. (2020) discusses how the sharing of information via cyberspace technologies to third parties and between public and private sector organisations creates a decentralisation and fragmentisation of the security of personal information with greater control being given to private security governance professionals. Neyroud and Disley (2008)

examine the impacts of electronic databases in relation to the concepts of fairness and legitimacy, arguing that the effectiveness of new technologies for detecting and preventing crime should not, and cannot, be separated from ethical and social questions surrounding the impact which these technologies might have upon civil liberties. They argue that this is due to the close inter-relationship between the effectiveness of the police and public perceptions of police legitimacy—which may potentially be damaged if new technologies are not deployed carefully. The authors argue that strong, transparent management and oversight of these technologies are essential, and suggest some factors to which a regime of governance should attend, including integrity and reliability of the technology, ensuring alignment between purpose and use in deployment of the technology, transparency in governance, and ensuring public confidence in the technology. Similarly, Vilendrer et al. (2021), use the example of data sharing from mobile applications between first responders during the Covid-19 pandemic in San Francisco in the United States to discuss concerns around the need for securing personal information. In contrast to the other documents that focus on the risks to privacy and human rights, McKendrick (2019) discusses how the storage and sharing of data in relation to countering terrorism may not have a deleterious effect on human rights, owing to greater abilities to protect citizens' right to life and the need to safeguarding against broader misuse of related technologies and data. McKendrick (2019) also argues broader access to less intrusive aspects of public data and direct regulation of how those data are used – including oversight of activities by private-sector actors – and the imposition of technical as well as regulatory safeguards may improve both operational performance and compliance with human rights legislation. However, they also note that it is important that measures proceed in a manner that is sensitive to the impact

on other rights such as freedom of expression, and freedom of association and assembly.

### c) Lack of Standardisation and Accountability

Five of the documents reviewed refer to how social and ethical concerns may arise as a result of a lack of standardisation between parties over data use and access and a lack of accountability (Henman 2019; Babuta and Oswald 2020; Sanders and Henderson 2013; Babuta 2017). For example, Henman (2019) explains that visions of greater efficiency, improved quality of service delivery and open and accountable government are often not achieved and how policy and administrative principles may be undermined due to increasing fragmentation and a lack of standardisation over procedures. Similarly, Babuta and Oswald (2020) note that there remains a lack of organisational guidelines or clear processes for scrutiny, regulation, and enforcement. They also add that this should be addressed as part of a new draft code of practice, which should specify clear responsibilities for policing bodies regarding scrutiny, regulation, and enforcement of these new standards.

### d) Differences in Organisational Practices

Three of the 15 documents reviewed examine the organisational barriers to information sharing and integrated policing (Henman 2019; Sanders and Henderson 2013; Baburta 2017). For example, Sanders and Henderson (2013) explore how differences in organisational practices can result in digital divides, leading to problems with data integration and a lack of standardisation in practice.

**e) Bias Embedded in Data, Data Organisation and Data Sharing Processes**

Three documents discussed the issue of the embedding of bias within electronic databases and the need for users to adopt a critical perspective towards the data being held (Weaver et al. 2021; Babuta 2017; Vilender et al., 2021). For example, Weaver et al. (2021) looks at tech-enhanced data sharing between police officers and psychiatric personnel for enhancing police referrals of individuals experiencing suicide crises into treatment and discuss the need for information to be both held and shared in a culturally sensitive way, acknowledging that data input and sharing can reflect the biases held by individuals. Similarly, Babuta (2017) acknowledges how data may contain existing biases and may reflect the over or under policing of certain communities and racial bias, which are then reproduced in the generated outcomes of the application of those datasets. Babuta (2017) also discusses how individuals from disadvantaged sociodemographic backgrounds are likely to engage with public services more frequently, meaning the police often have access to more data relating to these individuals, which may in turn lead to them being calculated as posing a greater risk in the application of that data.

### 3.1.1.2 Community Policing Applications

Sixteen of the 59 documents that examine electronic databases in relation to the social and ethical issues surrounding the use emerging technologies, discuss data storage from community policing applications (apps) and their use (Aston et al., 2021; Bloch 2021; Brewster et al., 2018; Davis and Garb 2020; Dunlop et al., 2021; O'Connor 2017; Van Eijk 2018; Weaver et al., 2021; Henman 2019; Ellis 2019; Goldsmith 2015; Hendrix et al., 2013; Gaelle and Joelle 2018; Hendl et al. 2020;

Henman 2019; Lum et al., 2017). Of these 16 articles, three themes emerged. These were:

- Risks of enhancing racial inequalities
- Issues of inclusion/exclusion and social and technological capital
- Maintaining public trust

### a) Risks of Enhancing Racial Inequalities

Two of the documents reviewed specifically address the issue of racism in relation to the storage of data from community policing applications (Bloch 2021; Hendrix et al. 2013). Bloch (2021) examines the use of the Nextdoor app as a means of community-instigated policing, which he argues embeds unchallenged racist attitudes in neighbourhood monitoring data. Hendrix et al. (2013) discuss community policing apps as part of broader community and hot spot policing strategies, noting that this can potentially result in enhancing hot spot policing and data gathering of particular geographic areas, which in turn, can potentially exacerbate inequalities in data of ethnic minority groups.

### b) Issues of Inclusion/Exclusion and Social and Technological Capital

One article discusses how the use of community policing application data can further the risk of exclusion between police and certain population groups owing to differences in the social and technological capital of those using the app and those being subject to monitoring (Brewster et al., 2018). Brewster et al. (2018) explains that the use of technologies in community policing represent a move away from reactive policing models towards those which establish a proactive philosophy, responsive to the wants and needs of communities. They also intend to help improve

the relationship and level of engagement between the police and the communities they serve. However, as they are often used more to disseminate information rather than to support communications in problem-solving, their effectiveness has been limited. In addition, they can be argued not to enhance public participation or community-police relations, but results in a widening gulf in participation and community-police relations owing to differences in social and technological capital between population groups, which results in inequalities between those who provide information and those whose information is being provided being recorded.

**c) Maintaining Public Trust**

Six of the documents reviewed discuss the issue of trust between community members and police in relation to the electronic information from community policing applications (Aston et al., 2021; Bloch 2021; Van Eijk 2018; O'Connor 2017; Ellis 2019; Lum et al 2017). For example, van Eijk (2018) discusses the coproduction of data in community-police applications and explores how the perceptions that citizens and professionals hold about each other's aims and engagement impact upon willingness to share information. Van Eijk (2018) argues that for greater two-way collaboration and trust to occur, transparency is needed about the aims of the engagement and how the data will be held. Lum et al. (2017) also explain that a lack of transparency may limit its potential to improve police-community relationships.

In contrast, O'Connor (2017) argues that by allowing people to communicate directly with the police as well as for information to be shared about matters like safety/traffic, community, and police activity in addition to specific matters of crime and investigation, these apps can help enhance trust between the police and

community. However, they also stress that consideration must be given to the visibility and storage of information to avoid damaging police-community relations. Aston et al., (2021) examine the issue of public trust and confidence amongst members of the public from minority groups in relation to online data in relation to online community policing data and show that key concerns raised surrounded the anonymity and privacy of information, risk of abuse of personal data and not having the option of opting out of having personal data stored.

#### 3.1.1.3: Data Pulling Platforms

Only two of the documents within the sample explored the social and ethical issues associated with data pulling platforms (Ellison et al., 2021; National Analytics Solutions 2017). Ellison et al (2021) explores how the utilisation of big data and its integration with administrative and open data sources and platforms can reflect inequalities in terms of police resources, which in turn influences its effectiveness and its outcome in terms of the interplay between policing demand and deployment. The National Analytics Solutions 2017 report explores the ethical implications associated with data pulling platforms and argues that one problem with these are that prisons, probation, education and health sectors, as well as civil society organisations, private industry, and communities have different cultures and practices regarding the collection, sharing, processing and use of different types of data, which in turn, can create shifts in distributions of power which then manifests in terms of data availability.

### 3.1.1.4: Social Media Platforms and Data Storage

Fourteen of the 59 documents that discuss electronic information and databases discuss the social and ethical implications associated with the collection, storage, management, and use of social media data in policing (Bullock 2018; Ellis 2019; Fussey and Sandhu 2020; Goldsmith 2015; Hendrix et al., 2019; Meijer and Thaens 2013; Oh et al. 2021; Todd et al., 2021; Walsh and O'Connor 2019; Williams et al., 2021; Williams et al, 2013; Veale 2019; Brabuta 2017; Strom 2017). Particular issues identified were:

- Issues of lack of alignment in organisational culture
- Issues surrounding legitimacy of police action
- The management and use of sensitive information
- Risks of enhancing actual and perceived social injustices

#### a) Lack of Alignment in Organisational Culture

Three of the documents discussed how the organisational culture affects how the collection, storage, management, and use of social media data is undertaken, exploring how lack of cooperation and standardisation between police departments and between police and third-party organisations as to how this should be conducted is a cause for concern (Bullock 2018; Hendrix et al., 2019; Meijer and Thaens 2013). For example, Bullock (2018) explains that social media has not helped to facilitate interaction between police and communities in the way that was desired in England owing to how the uses of social media data are mediated by existing organisational and occupational concerns of police departments. Similarly, Hendrix et al. (2019) argues that police use of social media data lacks clear guidance as to how it fits within its guiding philosophy and operational goals. Meijer and Thaens (2013)

explore how a lack of clear government policy or guidance for the collection, management and use of social media data poses a potential ethical risk as well as hinders its potential effectiveness in police practice.

**b) Legitimacy of Police Action**

Two articles discuss how the availability of social media data can be used to question and negotiate the legitimacy of police actions (Ellis 2019; Goldsmith 2015). Ellis (2019) examined the impacts of digital media technologies on police and lesbian, gay, bisexual, transgender, intersex, and queer (LGBTIQ) community relations in Sydney by examining how a viral video of police excessive force filmed after the 2013 Sydney Gay and Lesbian Mardi Gras parade raised questions about issues of legitimacy and procedural justice. She then discussed how social media data can be used to pressure the police to account for their actions and can lead to public questioning over what can be considered to be legitimate boundaries of police practice. Goldsmith (2015) examines the potential problems for police reputation, operational effectiveness and integrity of the criminal justice system that can arise from off-duty use of social media by police officers and the potential harm this can result in for community-police relations.

**c) Management and Use of Sensitive Information**

Four articles discuss the issues associated with sensitive information obtained specifically through social media data (Fussey and Sandhu 2020; Todd et al., 2021; Oh et al., 2021; Walsh and O'Connor 2019). For example, Fussey and Sandhu (2020) discuss the use of social media information in police surveillance activities as part of information gathering, digital forensics and covert online child sexual

exploitation investigations, and the ethical issues associated with extended surveillance and storage of data. Similarly, Todd et al. (2021) in their study of social media in relation to online stalking, domestic violence and homicide raised questions about the digital footprints of victims and perpetrators and their use criminal investigations and in responding to victims.

**d) Risks of Enhancing Actual and Perceived Social Injustices**

Two articles explored how the management and use of social media data posed a potential risk of exacerbating actual and perceived social injustices and tensions between police and community members (Williams et al., 2013; Walsh and O'Connor 2019). Williams et al. (2013) discuss how the Cardiff Online Social Media ObServatroy (COSMOS) affords users with the ability to monitor social media data streams for signs of high tension which can be analysed in order to identify deviations from the norm' (levels of cohesion/low tension), may potentially risk enhanced surveillance of particular community groups, which may negatively affect relations between police and these communities. Walsh and O'Connor (2019) explore how social media provides unprecedented capacities to monitor the police and expose, circulate, and mobilize around perceived injustice, whether brutality, racial profiling, or other forms of indiscretion.

### 3.1.1.5: Open-Source Data

Only four of the documents explored the social and ethical implications of the use of open-source data in relation to emerging technologies (Clavell et al., 2018; Ellison et al., 2021; Egbert and Krasmann 2020; Kjellgren 2022). Of these, one (Clavell et al. 2018) explores the social impact of open-source intelligence data by exploring how

this technology can result in increased victimisation if not adequately managed. Egbert and Krasmann (2020) explore how access to open-source data may 'drive' predictive policing strategies and sometimes unnecessary pre-emptive police action, while Ellison et al (2021) discusses the use of open data sources in relation to police demand. Finally, Kjellgren (2022) has considered how the application of big data analytics to open-source data associated with sex work and human trafficking, can disguise simplified conceptualisations of the problem leading both to over-policing and over-claiming regarding the scale of the issues being addressed.

#### *3.1.1.6: Vulnerable Population Databases and Datasets*

Nine of the documents reviewed explore the social and ethical implications of vulnerable population data in relation to developments in technology use in policing (Hendl et al., 2020; Lumsden and Black 2020; Malgiari and Niklas 2020; Powell and Henry 2018; Wolfe 2021; Brabuta 2017; Strom 2017; Whittelstone et al., 2019, National Analytics Solutions 2017). Three key issues were identified in the literature. These were:

- Opportunities and risks associated with surveillance of vulnerable populations
- Issues of human rights and justice
- The need for greater consultation and communication with vulnerable groups as to how data is stored and used
- Lack of guidance and prioritisation for data collection and management

**a) The Surveillance of Vulnerable Populations**

Six of the documents discuss the opportunities and risks associated with the potential of the enhanced surveillance of vulnerable populations through collection of

and access to data on vulnerable populations (Hendl et al., 2020; Whittelstone et al., 2019; Brabuta 2017; Strom 2017; Powell and Henry 2018; Wolfe 2021). Hendl et al. (2020) explains that in digital surveillance activities, vulnerable subpopulations pay a higher price for surveillance measures and that there are concerns that improperly restricted data availability could lead to the employment of disproportionate profiling, policing, and criminalization of marginalized groups. Wolfe (2021) examines the ethical issues associated with electronic data pertaining to missing people in police activity, while Whittelstone et al. (2019) explores the positive and negative implications of the enhanced holding of data of disadvantaged and underrepresented groups, such as women and people of colour, or vulnerable people such as children and older people, and argues that greater consideration needs to given to what tensions between values are more likely to arise and how they can be resolved. Brabuta (2017) discusses the implications of data storage and analytics that make it possible for police forces to use past offending history to identify individuals who are at increased risk of reoffending, as well as using partner agency data to identify individuals who are particularly vulnerable and in need of safeguarding. Storm (2017) discusses the issue of protecting vulnerable people from harm and explains how a lack of priority or guidance as to how and when information should or could be shared hinders effective management and deployment of vulnerable population data. Finally, Powell and Henry (2018) explore the use of vulnerable population data in relation to: (1) online sexual harassment; (2) gender and sexuality-based harassment; (3) cyberstalking; (4) image-based sexual exploitation (including revenge pornography'); and (5) the use of communications technologies to coerce a victim into an unwanted sexual act and address the challenges and promises of law enforcement in this area.

### b) Issues of Human Rights and Justice

Only one of the documents reviewed specifically addresses the issues of human rights and justice in relation vulnerable population data (Malgieri and Niklas 2020). Malgieri and Niklas (2020) explore how discussion and decision-making about vulnerable individuals and communities and the use of their data spread from research ethics to human rights. They explore how the development, deployment and use of data-driven technologies can pose substantial risks to human rights, the rule of law and social justice, and how the implementation of such technologies can lead to discrimination through the systematic marginalisation of different communities and the exploitation of people in particularly sensitive life situations. They argue for the special role of personal data protection and call for a vulnerability-aware interpretation. They also outline how the notion of vulnerability can influence issues of consent, Data Protection Impact Assessment, the role of Data Protection Authorities, and the participation of data subjects in the decision making about data processing.

### c) The need for Greater Communication with Vulnerable People as to how Data is Stored and Used

Two of the documents discuss the need for greater consultation and communication with vulnerable groups as to how data is collected, stored, and utilised in police practice, as well as for greater clarity around the issue of access to personal data (Malgieri and Niklas, 2020; Lumsden and Black, 2020). For example, Lumsden and Black (2020) discuss the importance of ensuring that data and services are

responsive to the needs of D/deaf citizens and argue that when designing police services and technologies, the focus must include the needs of D/deaf citizens.

**d) Lack of Guidance and Prioritisation for Data Collection and Management**

Two documents discuss the current lack of guidance and priorities for the collection, management, and use of vulnerable population data (Brabuta 2017; Strom 2017). Strom (2017) argues there should be an assessment to establish priorities and discusses how there are legal constraints on data processing and that some of these apply differently to law enforcement than to other parts of government services which are likely to be involved in data-sharing processes with vulnerable population in relation to law enforcement, such as social housing services. Babuta (2017) also explains that at present data-sharing deficiencies mean that the police's understanding of vulnerability is somewhat one-dimensional and argues that a clear decision-making framework should be developed at the national level to ensure the ethical use of vulnerable population data.

### 3.1.1.6: DNA databases

Four of the documents referred to social and ethical concerns associated with electronic databases storing information pertaining to human DNA (Custers and Vergouw, 2015; Gaelle and Joëlle, 2018; Neiva et al., 2022; Rigano, 2019). For example, Rigano (2019) explains that DNA analysis produces large amounts of complex data in electronic format that requires storage management. Gaelle and Joelle (2018) explore the production of ethical norms regulating biomedical practices and the importance of these for police work and management of genetic data.

### 3.1.2: Biometric Identification Systems

Fifty-five of the 173 documents in the final sample discussed the social and ethical implications of biometric identification systems in policing practice. The following specific types of biometric identification systems were discussed in the literature:

- Facial recognition technology, including 'remote' facial recognition technologies (17 out of 48 documents)
- Artificial intelligence, including AI smart sensors, automated algorithm processes and decision-making tools, and emotional recognition technologies (21 out of 55 documents)
- Voice pattern analysis tools (2 out of 55 documents)

#### 3.1.2:1: Facial Recognition Technologies

According to Chowdhury (2017), a number of terms are used to refer to facial recognition technology. These include automated facial recognition, live facial recognition (LFR) and facial recognition processes. Facial recognition technologies analyse an individual's face to determine identification in real time by examining facial patterns such as the distance between eyes and length of the nose in order to create facial templates and compare these to templates held on records. If the comparison results in a match a confidence score is produced. Thresholds for how strong or weak a match are set by the entity deploying the system (Chowdhury 2017). The matching process can be undertaken on a one-to-one matching basis where the system confirms that an image matches a different image of the same person in a record database or on a one-to-many basis where one image is compared to other records within a database.

Seventeen documents discussed the social and ethical implications associated with the implementation and use of facial recognition technologies (Almeida et al., 2021; Babuta 2017; Babuta and Oswald 2020; Bradford et al., 2020; Bragias et al., 2021; Bromberg et al., 2020; Chowdburg 2020; Fussey et al., 2021; Fussey and Murray 2019; Hood 2020; Keenan 2021; McGuire 2021; McKendrick 2019; National Physical Laboratory and Metropolitan Police Service 2020; Smith and Miller 2022; Urquhart and Miranda 2021; Williams 2020). Four key social and ethical issues were identified from this literature. These were:

- Trust and legitimacy
- Risk of enhancing inequalities for marginalised groups
- Privacy and security
- Lack of standardised ethical principles and guidance

**a) Trust and Legitimacy**

Five of the documents discuss how issues of trust and legitimacy manifest in relation to facial recognition technologies (Almeida et al., 2021; Bradford et al., 2020; Bragias et al., 2021; McGuire 2021; Williams 2020). Bradford et al., (2020) explores the results from a London-based study exploring public responses to Live Facial Recognition technologies which enable police to conduct real-time automated identity checks in public spaces. They argue that public trust and legitimacy are important factors in the acceptance and rejection of these technologies and highlight that high levels of trust and perceived legitimacy about the use of these technologies help to alleviate privacy concerns about their use. McGuire (2021) explains that perceptions of the potential misuse of these technologies and concern about the denial of rights can threaten the viability of policing and lead to questions about the

limits of the automation of policing. Bragias et al. (2021) explain that although facial recognition technologies offer a fast, efficient, and accurate way of identifying criminals, the public is often sceptical about how the police will use this technology and for what particular purposes. They argue that if police use of FRT is perceived as illegitimate, police-citizen relationships may deteriorate, especially for marginalised communities.

**b) Risk of Enhancing Inequalities for Marginalised Groups**

Five of the documents discuss how the use of facial recognition technologies pose particular social and ethical issues for police practice and relations with marginalised communities (Bragias et al. 2021; Chowdhury 2020; Hood 2020; Urquhart and Miranda 2021; Williams 2020). For example, Urquhart and Miranda (2021) discuss the results of an empirical and legally focused case study of live automated facial recognition technologies in British policing and discuss police concerns about how they may affect or be affected by anti-discrimination laws and how EU AI Regulation makes LFR a prohibited form of AI. Hood (2020) explores the integration of facial recognition into police body-worn camera devices and discusses the political dangers of these technologies. Hood argues that these technologies risk reinforcing normative understandings of the body and explores how facial recognition surveillance devices pose enhanced risks for marginalized groups and explains that body worn cameras with facial recognition devices present a number of socio-political dangers that reinforce the privilege of perspective granted to police in visual understandings of law enforcement activity and risk reinforcing racial marginalization. Similarly, Chowdhury (2020) argues that facial recognition technologies represent a form of monitoring technology which has a long history of being deployed primary

against people of colour. Chowdhury (2020) explains that people of colour are at substantially at risk of being over-policing and discusses how improvements in accurate facial recognition technologies will likely still exacerbate racial inequalities because it is highly likely that the technology will be disproportionately used against people and communities of colour, and uses the example of the London trials of this technology by the Metropolitan Police at the Notting Hill Carnival to highlight the inequalities of outcomes and to show the dangers resulting from failure to carry out an equality impact assessment before deploying this form of technology.

**c) Privacy and Security**

Eight of the documents reviewed discuss issues pertaining to privacy and personal security in relation to the deployment of facial recognition technologies (Almeida et al., 2021; Bragias et al., 2021; Keenan 2021; Smith and Miller 2022; Urquhart and Miranda 2021; Chowdhury 2020; Fussey and Murray 2019; National Physical Laboratory and the Metropolitan Police Service 2020). For example, Keenan (2021) explores how in the case of R (on the application of Bridges) v Chief Constable of South Wales Police, the Court of Appeal held that the deployment of live automated facial recognition technology (AFR) by the South Wales Police Force (SWP) was unlawful because it violated the right to respect for private life under Article 8 of the European Convention on Human Rights because it lacked a suitable basis in law. They also explored how the Data Protection Impact Assessment conducted under section 64 of the Data Protection Act 2018 failed to assess the risks to the rights and freedoms of individuals processed by the system. Similarly, Smith and Miller (2022) explain that biometric facial recognition technologies which involve the automated

comparison of facial features carry significant privacy implications that require law and regulation.

d) **Lack of Standardised Ethical Principles and Guidance**

Two of the documents explore the need for standard ethical principles and guidance to be introduced in order to help mitigate the social and ethical risks associated with facial recognition technologies (Babuta and Oswald 2017; Smith and Miller 2022). For example, Babuta and Oswald (2017) explain that there remains a lack of organisational guidelines or clear processes for scrutiny, regulation, and enforcement of biometric identification systems, including facial recognition technologies.

### 3.1.2.2: Artificial Intelligence

The term Artificial Intelligence (AI) is used to refer to any technology that performs tasks that might be considered to count as 'intelligent' in the sense that they replicate complex human cognitive processes and abilities in machines. These technologies can be used to optimise processes and can be designed and programmed to operate autonomously (Chowdhury 2019).

Twenty-one of the documents reviewed discuss the actual and potential social and ethical issues associated with Artificial Intelligence (AI) technologies in policing (Almeida et al., 2021; Aizerberg and van den Hoven 2020; Alikhademi et al., 2022; Asaro 2019; Beck 2021; Bradford et al., 2022; Dechesne 2019; Ellison et al., 2021; Ernst et al., 2021; Hayward and Maas 2021; Hobson et al., 2021; Noriega 2020; Smith and Miller 2022; Wright 2021; Grimond and Singh 2020; McKendrick 2019;

Whittelstone et al., 2019; Urquhart and Miranda 2021; Babuta 2017; Oswald 2019; Leslie 2019). Within these documents, the key social and ethical issues discussed are broadly focused on the following five key themes:

- Reproduction of systemic bias of human decision makers
- The need for ethical guidelines and laws for risk minimisation and improvements in efficiency potential
- Issues of accuracy, fairness, and transparency
- Specific risks of racial and gender bias
- Potential for use by perpetrators of crime

**a) Reproduction of Systemic Bias of human Decision Makers**

One article discusses the issue of the potential reproduction of systemic bias from human decision making in the deployment of artificial intelligence. Alikhademi et al., (2022) discusses the use of Artificial Intelligence in predictive policing and reveals how they are susceptible to replicating the systemic bias of previous human decision-makers.

**b) Accuracy, Fairness and Transparency**

Nine of the documents reviewed discuss the issues of accuracy, fairness and transparency associated with artificial intelligence in policing (Alikhademi et al., 2022, Whittelstone 2019; Smith and Miller 2022; Beck 2021; Veale 2019; Hobson et al., 2020; Asaro 2019; Wright 2021; McKendrick 2019). For example, Beck (2021) discusses the issue of fairness in relation to the use of artificial intelligence in law enforcement, predictive policing and risk assessment and explains that concerns about fairness are rooted upon concerns about the prospects of bias and an

apparent lack of operational transparency. Beck also shows how media coverage of the use of artificial intelligence can exacerbate these concerns but argues that potential solutions will be found through political and legislative processes that aim to achieve an acceptable balance between competing priorities. Hobson et al., (2021) focuses on the issue of fairness in relation to algorithmic policing and shows that members of the public tend to view a decision as less fair and appropriate when an algorithm decides compared to when a police officer decision and also shows how perceptions of fairness and appropriateness were strong predictors of support for police algorithms. They conclude that algorithm decision making may damage trust in the police, particularly in cases when the police rely heavily or solely on algorithmic decision making. Similarly, Asaro (2019) discusses the risks around the use of data-driven algorithms in policing and how this raises questions about fairness by effectively treating people as guilty of (future) crimes for acts they have not yet committed and may never commit, and how the use of predictive information systems may shape the decisions and behaviours of police officers.

### c) Risks of Racial and Gender Bias

Four documents discuss the potential risks associated with racial and gender bias in relation to Artificial Intelligence in policing (Noriega 2020; Asaro 2019; McKendrick 2019; Whittelstone 2019). For example, Noriega (2020) acknowledges how racial and gender bias may be embedded in the design and implementation of artificial intelligence technologies, however they also discuss the potential of artificial intelligence to promote a non-biased environment during police interrogation for mitigating racial and gender divides in statistics regarding false confessions.

**d) The Need for Ethical Guidelines and Law to Minimise Harm**

Nine of the documents discuss the need for clear, ethical guidelines and laws to minimise the potential harms associated with the use of artificial intelligence technologies in policing (Almeida et al., 2021; Asaro 2019; Bradford et al., 2022; Dechesne 2019; Ernst et al., 2021; Leslie 2019; Whittelstone 2019; Urquhart and Miranda 2021; Oswald 2019).

**e) Potential for Use by Perpetrators of Crime**

One article explores the potential risk of the application of Artificial Intelligence technologies by perpetrators of crime (Hayward and Maas 2021).

### 3.1.2.3: Voice Recognition Technologies

Two documents discuss social and ethical considerations of the use of voice recognition technologies in police practice (Lindeman et al. 2020; McKendrick 2019). Lindeman et al., (2020) explore how voice recognition technologies, as well as mobile, cloud, robotics and connected sensors are associated with concerns related to privacy and security and political and regulatory factors affecting interoperability, as well as concerns about a lack of standards. McKendrick (2019) also explains that voice recognition technologies are associated with concerns regarding human rights and a lack of well-established norms governing the use of AI technology in practice.

### 3.1.3: Surveillance Systems and Tracking Devices

Fifty-two of the 173 documents in the final sample discussed the social and ethical implications of surveillance technologies and tracking devices in policing practice.

The following specific types of these emerging technologies were discussed in the literature:

- Drones
- Smart devices and sensors
- Location and ‘Hot spot’ analysis
- Body worn cameras
- Autonomous security robots
- CCTV and visual/optical technologies

#### 3.1.3.1: Drones

Seven of the documents reviewed discuss the social and ethical implications associated with drone technology (Klauser 2021; Miliaikeala et al., 2018; Milner et al., 2020; Page and Jones 2021; Rosenfield 2019; Sakiyama et al., 2017; Wall 2016). The specific social and ethical issues associated with these forms of technology were:

- Legitimacy of use by police departments
- Issues of the development of an aerial geopolitics of security
- Public confidence and trust
- Concerns relating to racial bias
- Privacy

**a) Legitimacy of use by police departments**

One of the articles reviewed discusses the issue of the legitimacy of drone use by police departments in the United States (Miliakeala et al., 2018). They examine how unmanned aerial vehicles [UAVs or drones'] have come into routine police practices

and show that public attitudes toward police use of UAVs, and visual monitoring technology overall, is mixed owing to concerns about perceptions about police legitimacy and other criminal justice issues.

**b) Issues of the development of an aerial geopolitics of security**

Two articles example the issue of the development of a new aerial geopolitics of security as a result of the implementation of drones in security and policing (Klauser 2021; Milner et al., 2020). For example, Klauser (2021) explores the expectations and practices of new police drones in Switzerland to show how drones are transforming the ways in which the aerial realm is perceived within the context of policing, which has significant implications for power relations between the police and the public and for social governance.

**c) Public confidence and trust**

Five of the documents explore issues pertaining to public confidence and trust (Miliakeala et al., 2018; Milner et al., 2020; Page and Jones 2021; Rosenfield 2019, Sakiyama et al., 2017). For example, Milner et al., (2021) discuss how public opinion can affect the success of the use of these technologies and critically examine proposals for using drones to monitor political protests in the US.

**d) Concerns relating to racial biases in the deployment of these technologies**

Three articles discuss concerns relating to racial bias in the deployment of drones in police practice (Page and Jones 2021; Sakiyama et al., 2017; Wall 2016). For example, Page and Jones (2021) examine how in recent years US police departments have incorporated new aerial technologies that promise to make

policing more efficient and "race-neutral," including drones, which are positioned as unbiased and intended to function as an anti-emotional third-party witness to exchanges between the state and public. However, they found that the supposed accountability offered by these technologies does not upend the disciplining of emotion and examine how video footage demonstrates how ethnic minorities (especially women) regulate their emotional reactions to state violence both despite and because of the presence of these devices. Wall (2016) discusses the issue of state violence and routine police surveillance in the US which has gained recent attention as a result of the Black Lives Matter movement and argues that, if unregulated, these forms of technology, may increase the risks of accusations of state violence against minority groups when deployed in domestic policing contexts.

**e) Privacy**

Two of the documents discuss concerns relating to privacy in relation to the deployment of drones in policing practice (Sakiyama et al., 2017; Rosenfield 2019). Sakiyama et al., (2017) examines how the use of this form of technology, in general, and within the particular context of domestic policing activities, raises serious concerns about personal privacy and the greater intrusion of new forms of `big brother' surveillance in people's daily lives. They also examine socio-demographic differences in the public support for drone usage in this context. Rosenfield (2019) explains that the introduction of drones in the traffic enforcement context can lead to public acceptance challenges which can severely hinder their potential impact and discuss how privacy and safety are the main concerns expressed with regards to such technology in both the US and Israeli contexts.

### 3.1.3.2: Smart Devices and Sensors

Sixteen of the articles discussed social and ethical issues associated with the use of smart devices and sensors in policing (Braga et al., 2013; Brandt et al., 2021; Brewster et al., 2018; Catte et al., 2021; Ekabi et al., 2020; Joh 2019; Joyce et al., 2013; Kuo et al., 2019; Moon et al., 2017; Paterson and Clamp 2014; Sandhu and Fussey 2021; Stone 2018; Tulumello and Iapado 2021; Weaver et al., 2021; Whitehead and Farrell 2008; Urquhart, Miranda and Podoletz, 2022). Two overarching key ethical issues were identifiable within this body of literature. These were:

- The issue of privacy
- Trust and legitimacy of police use

#### a) Privacy

Seven of the articles discussed the issue of privacy in relation to the use of smart devices and sensors in relation to police activities and investigations. For example, Joh (2019) explain that as policing becomes increasingly ‘smarter’, concerns regarding the level of increased surveillance that highly networked systems pose are rising. They also discuss how these devices mean that police services will be required to spend more time watching the outputs of these devices and will also have less freedom themselves from being watched.

#### b) Trust and legitimacy of police use

Four of the articles spoke to the issue of trust and the legitimacy of police use in relation to the deployment of these devices (Moon et al., 2017; Joyce et al., 2013; Paterson and Clamp 2014; Braga and Schnell 2013). For example, Joyce et al.,

(2013) examine how the introduction of smart policing initiatives requires ongoing collaboration with both the public and with researchers to maintain trust.

### 3.1.3.3: Location and 'Hot Spot' Analysis Tools

Four of the documents reviewed discuss the social and ethical issues relating to location and hot spot analytical technologies (Koper et al., 2015; Nellis 2014; Braga and Schnell 2013; Hendrix et al., 2013). Key issues identified were:

- Effectiveness in reducing crime
- Challenges concerning the legitimacy of product selection
- Lack of guidance or integration of technology within specific crime reduction agendas

#### a) Effectiveness in reducing crime

Two of the documents discussed the effectiveness of these technologies in actually reducing crime (Koper et al., 2015; Braga and Schnell 2013). Koper et al. (2015) examined the use of mobile technology in hot spot policing in the US and found that officers used these technologies primarily for surveillance and enforcement (e.g., checking automobile license plates and running checks on people during traffic stops and field interviews), but not for strategic problem-solving and crime prevention and concluded that the applications of mobile computing may have little if any direct, measurable impact on officers' ability to reduce crime in the field. Braga and Schnell (2013) examined the Boston Police Department's implementation of the Safe Street Teams program to control "hot spots" using a Smart Policing Initiative to assess its ability to prevent violent crime.

**b) Challenges concerning the legitimacy of product selection**

One article (Nellis 2014) discussed how England and Wales have been privatizing its probation service and creating an advanced electronic monitoring scheme using combined GPS tracking and radio frequency technology. Nellis (2014) examines how providers of these technologies had been overcharging the government for their services, resulting in a series of enquiries and concerns about the legitimacy of the adoption of these technologies.

**c) Lack of guidance or integration of technology within specific crime reduction agendas**

One article raises concerns over the issue that police departments may adopt these technologies without giving proper consideration to how this form of technology fits within their guiding philosophy or operational goals (Hendrix et al., 2019).

### 3.1.3.4: Body Worn Cameras

Twenty-three of the documents reviewed discussed the social and ethical implications associated with body worn cameras (Lum et al. 2017; White et al., 2018; Ariel et al., 2015; Saulnier et al., 2020; Smykla et al., 2016; Huff et al., 2018; Miranda 2022; Todak et al., 2018; Backman and Lofstrand 2021; Stalcup and Helm 2016; Bromberg et al., 2020; Stone 2018; Cuomo and Dolci 2021; Gramagila and Phillips 2018; Hamilton-Smith et al., 2021; Healey and Stephens 2017; Henne et al., 2021; Miliaikaela et al., 2018; Hood 2020; Murphy and Estcourt 2020; Page and Jones 2021; Ray et al., 2017; Sahin and Cubukcu 2021). The following different types of social and ethical issues were highlighted within this body of literature:

- Implications for public-state relationships

- Impacts on police officers and police practice
- Concerns about racial biases inherent in deployment of the technology

**a) Implications for public-state relationships**

Eleven of the documents discussed the impacts of these technologies for public-state relationships (White et al., 2018; Saulnier et al., 2020; Todak et al., 2016; Hamilton-Smith et al., 2021; Healey and Staples 2017; Lum et al., 2019; Ariel et al., 2015; Brockman and Lofstrand 2021; Bromberg et al., 2020; Murphy and Estcourt 2020; Smykla et al., 2016). For example, Ariel et al., (2015) examined the effects of body worn on cameras on complaints against the police, while Hamilton-Smith et al., (2021) examined the interplay of police techniques and surveillance technologies in the policing of Scottish football. They found that that several practices were considered intimidatory and argued that the use of technologies such as powerful hand-held cameras and body worn video (BWV) has had a detrimental impact on police-fan relationships, interactions, and dialogue. Murphy and Estcourt (2020) examine concerns around privacy in relation to body-worn cameras in both the Australian and US contexts.

**b) Impacts on police officers and police practice**

Four of the documents discuss the impacts of body worn cameras for members of the police service as well as on policing practice (Gramagila and Phillips 2018; Henne et al., 2021; Huff et al., 2018; Miranda 2022). For example, Gramagila, and Philips (2018) found that police officers in the US and UK wanted to have the ability to be able to review body camera images prior to writing a report, while Henne et al., (2021) discuss how the introduction of body worn cameras by police officers has

been a popular response to public demands for greater police accountability, particularly in relation to racially marginalised communities and argue that the use of body worn cameras redefines police violence into a narrow conceptualisation rooted in encounters between citizens and police and can direct attention away from the structural conditions and institutions that perpetuate police violence. Miranda (2022) discusses the challenges that have been faced during the implementation of this form of technology in the UK police force context to identify the practical and techno-social challenges associated with these technologies and the interrelationships between these types of challenges. They conclude that use of these cameras and how they operate technically are connected, which raises significant ethical issues for data management and storage.

**c) Concerns about racial biases inherent in deployment of the technology**

Two articles discuss concerns about racial biases and inequalities in relation to the deployment of these forms of technology (Murphy and Estcourt 2020; Hood 2020). Murphy and Estcourt (2020) explain how the use of body worn cameras and other surveillance devices may contribute to the over-surveillance of minority communities. Similarly, Hood (2020) explores how these technologies may result in a leveraging political power and racial marginalization.

### 3.1.3.5: Autonomous Security Robots

Only one of the documents reviewed referred to the issues associated with autonomous robots in relation to policing practice. Asaro (2019) considers the ethical challenges facing the development of robotic systems that can potentially deploy violent and lethal force against humans. Although the use of violent and lethal force

is not usually acceptable, police officers are authorized 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. With the increased interest in developing and deploying robots for law enforcement tasks, including robots armed with weapons, Asaro (2019) discusses the problem of design human-robot interactions (HRIs) in which violent and lethal force might be among the actions taken by the robot.

### 3.1.3.6: CCTV and Visual/Optical Technologies

Six of the documents within the sample discuss the social and ethical issues associated with Closed Circuit Television and other Visual/Optical forms of Technology (Aston et al., 2022; Dunlop et al., 2021; Miliakeala et al., 2018; Brockman and Jones 2022; Clavell et al., 2018, Lauf and Borrion 2021). For example, Dunlop et al., 2021 examine how these forms of technology play an important role in preventing and responding to hate crime, which can improve police-community relationships. However, in their review of the use of CCTV in British homicide investigations, Brookman and Jones (2022) argue that although CCTV is used more frequently than any other kind of forensic science or technology to both identify and charge suspects, particular challenges are associated with how CCTV footage is recovered, viewed, shared, interpreted, and packaged for court. In particular, the lack of clear standards and principles can be especially problematic. Clavell et al., (2018) argues that if these technologies are not managed correctly, they can result in increased victimization, inequalities, or inefficiency. Aston et al., (2022) examine the use of mobile devices by the police and the public using the concept of the ‘abstract police’ to consider the impact of mobile surveillance

technologies on legitimacy between members of the public and the police, as well as internally within police departments.

**Table 1** shows a summary of the findings of the social and ethical issues associated with each type of technology.

With the key social and ethical considerations associated with the various types of emerging technologies having been identified in this sub-section, the next sub-section will focus on the legal considerations associated with the adoption of emerging technologies in policing.

**Table 1 - Summary of Findings: Social and Ethical Issues Associated with Emerging Technologies by Technology Type and Specific Technology**

| Technology Type | Specific Technology | Associated Social and Ethical Issues |
|---|---|---|
| Electronic Databases | Data Sharing and Third-Party Data Sharing Technologies | • Safety of Information Held<br>• Human Rights and Privacy<br>• Lack of Standardisation & Accountability<br>• Differences in Organisational Practices<br>• Bias Embedded in Data Storage Practices |
| | Community Policing Application Data | • Risk of Enhancing Racial Inequalities<br>• Issues with Exclusion and Social and Technological Capital<br>• Maintaining Public Trust |
| | Data Pulling Platforms | • Reflective of Inequalities in Policing Resources<br>• Reflective of Unequal Distribution of Power between Different Policing Organisations |
| | Social Media Application Information | • Lack of Alignment in Organisational Culture<br>• Legitimacy of Action<br>• Management and Use of Sensitive Data<br>• Risk of Enhancing Social Injustices |
| | Use of Open-Source Data | • Risk of Increased Victimisation<br>• Risk of Unnecessary Pre-Emptive Police Action & Over-Policing |
| | Vulnerable Population Data | • Risk of Over-Surveillance of Vulnerable Populations<br>• Human Rights and Justice<br>• Questions over the Need for Consultation & Communication with Vulnerable Groups on How Data will be Stored and Used<br>• Lack of Guidance for Data Collection and Management |
| | DNA Databases | • Issues Arising from Poor Storage Management<br>• Lack of Ethical Norms regarding Storage of Biomedical Data |
| Biometric Identification Systems | Facial Recognition Technologies | • Trust and Legitimacy<br>• Bias Against Marginalised Groups<br>• Privacy and Security<br>• Lack of Standardisation, Ethical Principles and Guidelines |
| | Artificial Intelligence | • Reproduction of Systemic Bias of Human Decision-Making<br>• Lack of Ethical Guidelines for Risk Minimisation |

| | | |
|---|---|---|
| | | • Use by Perpetrators of Crime |
| | Voice Pattern Analysis Tools | • Privacy and Security<br>• Lack of Standards and Established Norms |
| Surveillance Systems & Tracking Devices | Drones | • Legitimacy of Use by Police<br>• Development of an Aerial Politics of Security<br>• Racial Bias & Privacy |
| | Smart Devices and Sensors | • Trust and Legitimacy<br>• Concern over Privacy and Risk of Over-Policing of Certain Groups |
| | Location and Hot Spot Analysis | • Questionable Effectiveness in Reducing Crime<br>• Challenges over Legitimacy of Product Selection<br>• Lack of Guidance for Integration in Crime Reduction Agendas |
| | Body-Worn Cameras | • Implications for Public-State Relationships<br>• Racial Bias |
| | Autonomous Security Robots | • Potential Use of Violence and Force Against Humans |
| | CCTV & Visual/Optical Technologies | • Lack of Standards for how Footage is Retrieved, Viewed and Stored<br>• Risk of Increased Victimisation<br>• Questions of Legitimacy |

## 3.2: Legal Considerations Associated with the Adoption of Emerging Technologies in Policing

UK case law identified as relevant to the adoption of emerging technologies in policing is set out in **Appendix 3.** International case law considered to be relevant is set out in **Appendix 4** and **Appendix 5** sets out the key provisions of significant legislation, the technologies to which they may apply and, if available, cites the relevant case law addressing that legislative provision. **Appendix 5** can be used as a useful tool against which to evaluate the legal issues/considerations that may be presented by a specific piece of emerging technology.

### 3.2.1: The Law of Evidence and Emerging Technology

#### 3.2.1.1: Improperly obtained evidence

Evidence can be obtained in a number of ways including search of premises, search of persons, search of personal property, taking of biological samples and the use of surveillance technologies. In each case for such evidence to be considered 'legally obtained' it must comply with the rules of evidence. Where it does not do so, evidence will be considered to have been obtained improperly. Where information is improperly obtained its admissibility can be questioned. The common law rule is that the admissibility of improperly obtained evidence is a balancing exercise considering on the one hand, 'the interest of the citizen to be protected from illegal or irregular invasions of his liberties by the authorities' and on the other 'the interest of the State to secure that evidence bearing upon the commission of crime and necessary to

enable justice to be done'.[5] Importantly, it has been recognised that such evidence should not be 'withheld from the Courts of law on any merely formal or technical ground.'[6] In addition to the possible challenges in terms of admissibility, where information is improperly obtained, the most likely ground 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.[7]

Beyond the common law principles, there are statutory forms of regulation that will impact on the construction of whether or not intelligence or evidence has been legally obtained. These would include the 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 prospectively the Scottish Biometric Commissioners' Code of Conduct.[8]

The use of emerging technologies is highly likely to challenge the boundaries of these legislative measures.[9] For example, the Criminal Procedure (Sc) Act 1995 s18(3) requires that all records of physical data, taken from an individual in custody, be destroyed as soon as possible, when it is decided proceedings are not to be raised, or do not conclude in a conviction. If Police Scotland were to consider the

[5] Lawrie v Muir 1950 JC 19 at 26.
[6] Lawrie v Muir 1950 JC 19 at 26.
[7] 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)
[8] Scottish Biometrics Commissioner: National Assessment Framework for biometric data outcomes, January 2022 and s7, Scottish Biometrics Commissioner Act 2020. asp 8.
[9] 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.

development of a specific biometric database or the deployment of technologies that are dependent on such data, they have to consider how such a database is to be populated and adopt an appropriate destruction policy that complies with s18.

The regulation of prints and samples is addressed in s18-20 of the CPSA 1995. These provisions provide lawful authority for the retention and use of such samples including use of any data derived from those samples.[10] Accordingly, where any emerging technology is used for the purposes of cataloguing, analysing, or storing such data consideration must be given to these provisions. The Code of Practice issued by the Scottish Biometrics Commissioner has the potential to address the ambiguity surrounding the boundaries of such provisions and is to be welcomed.[11]

Recently, and 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.[12] These provisions should offer clarity on the process to be followed and the limitations on the extraction of information. Data can be extracted, if a device is voluntarily provided, for the purposes of preventing, detecting, investigating, or prosecuting crime, helping to locate a missing person, or protecting a child or an at-risk adult from neglect or physical, mental, or emotional harm.[13] Importantly, there are restrictions on the

[10] S v United Kingdom (30562/04); Marper v United Kingdom (30566/04) [2008] 12 WLUK 117
[11] S7(3), Scottish Biometrics Commissioner Act 2020. asp 8. The Code of Practice can be accessed here: Code of Practice | Scottish Biometrics Commissioner.
[12] 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.
[13] Section 37(2) The Police, Crime, Sentencing & Courts Act 2022.

scope of these purposes. For example, the authorised person must reasonably believe that information stored on the electronic device is relevant to a reasonable line of enquiry which is being, or is to be, pursued by an authorised person.[14] Further, if the extraction of data is likely to include data beyond that relevant to the specific issue, there should be a test of proportionality.[15] In addition, the authorised person should ensure they are compliant with the Code of Practice.[16] There are significant protections offered to children in that those under 18 do not have capacity to consent to the extraction of data from their devices. The implication of this is that an authorised person would have to establish the age of the person consenting in order to ensure the legality of any subsequent extraction of data.[17]

#### 3.2.1.2: Disclosure of evidence

Part 6 of the Criminal Justice & Licensing (Sc) Act 2010 set out the rules of disclosure. Those rules require that an investigating agency provide all information relevant to a case for or against the accused that the agency is aware of, that was obtained in the course of investigating.[18] In addition, if requested to do so by the prosecutor, the investigating agency must provide the prosecutor with any of that specific information.[19] Here, information is defined as any 'material of any kind'.[20] This is important in the context of emerging technologies because when designing or selecting those technologies, consideration should be given to if, and how,

[14] Section 37(5)(a) The Police, Crime, Sentencing & Courts Act 2022.
[15] Section 37(7) The Police, Crime, Sentencing & Courts Act 2022.
[16] A specific code of practice is to be developed in terms of Section 42, The Police, Crime, Sentencing & Courts Act 2022.
[17] The protection of children is a recurring theme in the context of citizen-police relationships and merits specific attention.
[18] S117(2) (Solemn proceedings), s119(2) (Summary) Criminal Justice & Licensing (Sc) Act 2010.
[19] S117(3) (Solemn proceedings), s119(3) (Summary) Criminal Justice & Licensing (Sc) Act 2010.
[20] S116 Criminal Justice & Licensing (Sc) Act 2010.

information can be shared with the Crown Office & Procurator Fiscal Service so that they can comply with their obligation to disclose information to the defence.[21] A failure to do so at an early stage may impact on the ability of the police to comply with the rules of disclosure. Cases could be challenged on the basis of the prejudicial effect of that information not being made available.[22] This is likely to present a particularly acute problem as automated decision-making systems, artificial intelligence and ultimately algorithm become more embedded in policing practice and since the transparency of such systems is problematic[23]

At the international level, measures are being developed that seek to facilitate the disclosure of electronic evidence. This has most recently taken the form of a Protocol to the Cybercrime Convention.[24] Although the UK is not a signatory, at this point in time, it will enter into force once there are five ratifications. The protocol seeks to enhance cooperation between states to ensure that offences recognised by the cybercrime convention (such as illegally accessing a computer system, data interference, misuse of devices etc) can be effectively investigated and prosecuted.[25] It goes so far as to require that parties introduce domestic legislation that facilitates the disclosure of personal information from providers of domain name registration services.[26] It also requires that parties introduce domestic measures that facilitate

[21] S121(2) Criminal Justice & Licensing (Sc) Act 2010.
[22] Henderson (Colin) v Her Majesty's Advocate [2017] HCJAC 43 at para 23.
[23] 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.
[24] Second Additional Protocol to the Convention on Cybercrime on enhanced cooperation and disclosure of electronic evidence Strasbourg, 12.V.2022
[25] Council of European, Convention on Cybercrime Budapest, 23.XI.2001, Chapter II.
[26] Article 6(1), Second Additional Protocol to the Convention on Cybercrime on enhanced cooperation and disclosure of electronic evidence Strasbourg, 12.V.2022

the sharing of subscriber information[27] While not specifically focused on police-citizen relationships per se, if does form part of the framework that facilitates the lawful basis on which evidence can be exchanged and this in turn will impact on the transparency, accountability, and the connected trust the police service are able to foster.[28] In both cases of improperly obtained evidence and failures in the disclosure of evidence there is the potential to erode public trust in the police service.

**Recommendation**

Compliance with the law of evidence and the rules of disclosure will impact on the lawfulness of evidence, its admissibility, and the protection of rights (specifically Article 6 Right to a Fair Trial and Article 8 Right to privacy). Therefore, at the outset of designing, adapting, or adopting an emerging technology consideration should be given to how that technology is to be used. This means identifying whether that technology is being used to collect evidence or intelligence and whether it is being used is an overt or covert manner so that the appropriate procedural law can be complied with.

### 3.2.2: Data Protection

The Data Protection Act 2018 sets out the principles that must be complied with in the processing of 'personal data'. Part III specifically sets out the regulation of personal data in the context of law enforcement processing. There are additional safeguards required when such processing includes sensitive processing.[29] That includes processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership; (b) the processing of genetic data, or of biometric data, for the purpose of uniquely

[27] Article 7(1), Second Additional Protocol to the Convention on Cybercrime on enhanced cooperation and disclosure of electronic evidence Strasbourg, 12.V.2022

[28] Tyler, T, Yuen, J. Huo. Trust in the Law: Encouraging Public Cooperation with the Police and Courts (Russell Sage Foundation, New York, 2002)

[29] S42 Data Protection Act 2018.

identifying an individual; (c) the processing of data concerning health; (d) the processing of data concerning an individual's sex life or sexual orientation.[30] It is highly likely that many of the emerging technologies will involve such processing.

Of particular relevance in the context of emerging technologies, there is a prohibition on the use of automated processing as the sole foundation of decision making.[31] This prohibition only applies where the decision is a 'significant' one, which means either it 'produces an adverse legal effect concerning the data subject' or 'significantly affects the data subject'.[32] In order to be able to use automated processing as the sole foundation of decision making it must be authorised by law and 'the controller must, as soon as reasonably practicable, notify the data subject in writing that a decision has been taken based solely on automated processing.'[33]

An integral part of complying with the provisions of the data protection framework is that there needs to be a clear mapping of what and how data is being processed. In addition, in order for that processing to be lawful, there is a need to have an appropriate policy document in place.[34] The second data protection principle is likely to play an important part in the assessment of emerging technologies since it requires that where data is being collected for law enforcement purposes those purposes are 'specified, explicit' and 'legitimate' and that data must not be processed for an incompatible purpose.[35] The legislation expressly prohibits the processing of

[30] S35(8) Data Protection Act 2018.
[31] S49 Data Protection Act 2018.
[32] S49(2) Data Protection Act 2018.
[33] S50 Data Protection Act 2018.
[34] Data Protection Act 2018, Section 35.
[35] Data Protection Act 2018, Section 36(1)

data for non-law enforcement purposes unless it is authorised by law.[36] Within the legislation 'law enforcement purposes' is given a narrow definition of 'the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security'.[37] For example, this would not encompass the processing of data relating to an individual who is a missing person (unless it involved the assertion of either a criminal offence having been committed or that the individual presents a public security risk).

Since it is well recognised that police are often engaged in activities considerably beyond the scope of this narrow definition, Police Scotland would have to ensure that there is an appropriate 'authorisation in law for that processing'. In the context of the use of emerging technologies, where this is likely to be important is in the interaction between private sector organisations who may be engaged in facilitating the development of the technology or providing services to those involved in policing. Of particular importance will be the restriction on the use of data for development of the technology itself or the sharing of data with third parties. We already have a number of warning cases in the design and implementation of cyberkiosks, the development of track and trace apps for the purposes of public health and the use of biometric identification services provided by commercial entities. Each of these examples is addressed further below (Section 3.5)

[36] Data Protection Act, Section 36(4).
[37] Data Protection Act 2018, Section 31.

Again, the automation of aspects of data processing is likely to present challenges for compliance with the data protection principles set out in Part III. This is because as artificial intelligence progresses there may be difficulties the accountability and transparency of its operation. With this in mind, it will be necessary to ensure that appropriate procedures and in place to ensure consideration is given to whether where there is ambiguity in the quality, reliability, or transparency in how data is being processed by automated means.

**Recommendation**

In order to ensure robust data protection compliance:

1. Data protection policies should be kept under regular review to ensure that they capture the development and use of emerging technologies in the context of policing
2. A data impact assessment (DPIA) should be carried out prior to the development of any emerging technology (and revised as it progresses through from trial to deployment)

3.2.3: Equality and Human Rights

This report has focused on the use of emerging technologies in the context of police-citizen interactions. Careful consideration must be given to the characteristics of the affected citizen/citizen group that may present additional legal and ethical questions. For example, where the emerging technology is to be deployed in a context involving children (defined as those under 18), steps will have to be taken to ensure compliance with the United Nations Convention on the Rights of the Child. Following a ruling of the Supreme Court in October 2021 issues were raised concerning the constitutional validity of the Scottish Parliaments' attempt to incorporate the

convention into domestic law.[38] However, it is the intention of the Scottish Government to pursue implementation. The consequences of this are as yet unclear and merit a specific piece of research that can fully explore how children rights may be affected by the implementation of emerging technologies in the context of policing and how those rights can be appropriately secured.

| **Recommendation** |
| --- |
| Further research required 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. |

As it stands, public authorities are bound by the public sector equalities duty set out in section 149 Equality Act 2010. The scope of this duty is that they "must, in the exercise of its functions, have due regard to the need to:

(a) eliminate discrimination, harassment, victimisation, and any other conduct that is prohibited by or under this Act.

(b) advance equality of opportunity between persons who share a relevant protected characteristic and persons who do not share it.

(c) foster good relations between persons who share a relevant protected characteristic and persons who do not share it."[39]

The definition of public authority includes the Scottish Biometrics Commissioner[40], the Scottish Police Authority[41], the Chief Constable of the Police Service of

[38] Reference by the Attorney General and the Advocate General for Scotland - United Nations Convention on the Rights of the Child (Incorporation) (Scotland) Bill [2021] UKSC 42

[39] Section 1 (1), Equality Act 2010.

[40] Scottish Biometrics Commissioner | What We Do | Scottish Biometrics Commissioner.

[41] Home of Scottish Police Authority - Scottish Police Authority (spa.police.uk).

Scotland.[42] As a result, when considering the introduction of emerging technologies public authorities engaged in determining policing policy and practice need to consider if the deployment of that technology complies with this public sector equality duty.[43] It should perhaps be acknowledged that the jurisprudence of the Courts determines that this does not mean that there has to be an equality impact assessment in order to discharge this duty.[44] Nor does it suggest that a 'box-ticking' exercises will necessarily secure compliance with the duty.[45] Rather the focus is on the substance and circumstances of what has occurred. Ultimately, asking whether 'due regard' was given. That being said, it is clear that from a practical perspective conducting an equality impact assessment is likely to be one mechanism to support organisations in ensuring that 'due regard' is had and evidencing that. While these considerations are mainly matters of governance, sight should not be lost of the fact that the deployment of emerging technologies without such consideration has the potential to exacerbate discrimination, harassment, and victimisation.[46] For example, this reality can be seen in the concerns raised in the deployment of facial recognition technologies discussed below (Biometric Identification Systems).

All emerging technology used in a policing context will have the potential to impact on human rights. It is possible that technologies may support human rights protection. For example, if police officers were to have access to real time translation, they would be able to support the Article 6 right to a fair trial by providing

[42] Schedule 19 Equality Act 2010.
[43] R (on the application of Bridges) v Chief Constable of South Wales [2020] EWCA Civ 1058
[44] R. (on the application of Brown) v Secretary of State for Work and Pensions [2008] EWHC 3158; [2009] PTSR 1506, at paragraph 89.
[45] Haque v Hackney London Borough Council [2017] EWCA Civ 4, at paragraph 86.
[46] Artem Domnich and Gholamreza Anbarjafari, Responsible AI: Gender bias assessment in emotion recognition, arXiv:2103.11436v1 [cs.CV] 21 Mar 2021.

information promptly on the nature and cause of the accusation against them.[47] However, there are equally many concerns with the potential negative impacts.[48]

The majority of legal challenges to the deployment of new technologies have been framed in terms of the Article 8 right to privacy.[49] Examples of these challenges are cited where relevant in the discussion below.

#### 3.2.3.1: Databases

The legal regulation of the design and operation of databases is dictated predominantly by the Data Protection Act 2018. The key provisions likely to be triggered by emerging technologies are set out in the table of legislation in **Appendix 5**. In the main, the key factor is to determine whether a database concerns the processing of personal data and whether that data is of a sensitive nature as this assessment will determine if it is regulated by the DPA and if yes, how.

In the UK, to date, the use of databases has been challenged on the basis that they breach data protection law and that inclusion of personal data on them is ultimately an infringement of Article 8 ECHR. These challenges have related to three specific

[47] Article 6(3)(a), European Convention on Human Rights.
[48] Aston, V., "State surveillance of protest and the rights to privacy and freedom of assembly: a comparison of judicial and protester perspectives", in European Journal of Law and Technology, Vol 8, No 1, 2017. Council of Europe, Guidelines on artificial intelligence and data protection adopted by the Committee of the Convention for the Protection of Individuals with regards to Processing of Personal Data (Convention 108) on 25 January 2019. Section 1.4. p8.
[49] European Court of Human Rights, Factsheet: New Technologies. April 2022. Available: FS_New_technologies_ENG (coe.int).

aspects whether the data should be retained, for how long, and at what point should it be deleted.[50]

### 3.2.3.2: Biometric Identification Systems

In many respects there is overlap between the regulation of databases and the operation of biometric identification systems. By and large such systems will be operationalised through the use of a database of some kind. However, the key issue here is that biometric information is inherently sensitive personal information and so demands greater protection. Biometric data has most recently been given a statutory definition as "information about an individual's physical, biological, physiological, or behavioural characteristics which is capable of being used, on its own or in combination with other information (whether or not biometric data), to establish the identity of an individual, and may include: (a) Physical data comprising or derived from a print or impression of or taken from an individual's body, (b) A photograph or other recording of an individual's body or any part of an individual's body, (c) Samples of or taken from any part of an individual's body from which information can be derived, and (d) Information derived from such samples."[51]

[50] AS1's (A Child) Application for Judicial Review, Re [2021] NIQB 11, R (on the application of Bridges) v Chief Constable of South Wales [2020] EWCA Civ 1058, R (on the application of C) v Commissioner of Police of the Metropolis [2012] EWHC 1681 (Admin), R (on the application of Catt) v Association of Chief Police Officers of England, Wales and Northern Ireland [2015] UKSC 9, R. (on the application of II) v Commissioner of Police of the Metropolis [2020] EWHC 2528 (Admin), R (on the application of M) v The Chief Constable of Sussex Police, Brighton & Hove [2021] EWCA Civ 42, R (on the application of Miller) v College of Policing [2021] EWCA Civ 1926, R (on the application of the National Council for Civil Liberties (Liberty)) v Secretary of State for the Home Department [2019] EWHC 2057 (Admin), R (on the application of Wood) v Commissioner of Police of the Metropolis [2009] EWA Civ 414 (See appendix 3 UK Case Law table for case law summaries). Also see Big Brother Watch v United Kingdom (58170/13) [2018] 9 WLUK 157, Gaughran v United Kingdom (45245/15) [2020] 2 WLUK 607, Liberty v United Kingdom (58243/00) [2008] 7 WLUK 25, RE v United Kingdom (62498/11) [2015] 10 WLUK 707 , S v United Kingdom (30562/04); Marper v United Kingdom (30566/04) [2008] 12 WLUK 117 (See appendix 4 International Case Law for case law summaries).

[51] Scottish Biometrics Commissioner Act 2020, Section 34.

As noted earlier, Scotland has its own Biometrics Commissioner. Their role is to "to support and promote the adoption of lawful, effective and ethical practices in relation to the acquisition, retention, use and destruction of biometric data for criminal justice and police purposes".[52] In April 2022, they issued their draft Code of Practice. [53] The Guiding Principles and Ethical Considerations are set out in the box below.

The code of practice applies to Police Scotland, The Scottish Police Authority, and the Police Investigations and Review Commissioner. When acquiring, retaining, using, or destroying biometric data, these authorities must ensure compliance with this code of practice (once finalised).[54]

**Draft Code of Practice On the acquisition, retention, use and destruction of biometric data for criminal justice and police purposes in Scotland (April 2022)**

**Guiding Principles and Ethical Considerations**

1. Lawful Authority and Legal Basis
2. Necessity
3. Proportionality
4. Enhance public safety and public good
5. Ethical behaviour
6. Respect for the human-rights of individuals and groups
7. Justice and Accountability
8. Encourage scientific and technological advancement
9. Protection of children, young people, and vulnerable adults
10. Promoting privacy enhancing technology
11. Promote Equality
12. Retention periods authorised by law

[52] Scottish Biometrics Commissioner Act 2020, Section 2(1).

[53] Code of Practice | Scottish Biometrics Commissioner [Accessed 6 June 2022]. The code of practice applies to the computerised data as well as to raw physical samples (e.g. blood, saliva etc).

[54] Biometric data relating to national security issues will be addressed by the UK Biometric and Surveillance Camera Commissioner in accordance with s20 of the Protections of Freedoms Act 2012.

Although a failure to comply with the code will not in itself give rise to grounds for legal action, compliance with the code must be taken into account by a Court or tribunal in any proceeding whether civil or criminal to which the code may be relevant.[55] What this means in practical terms is that it must be taken into account in deciding whether evidence has been improperly obtained, or for example, in disciplinary proceedings in relation to a specific officer's professional conduct.

As with the introduction of any code of practice, it will be necessary to ensure that those engaged in the biometric data supply chain are given appropriate training.

The collection and use of biometric data (in the form of facial recognition) has faced significant judicial attention in the English and Welsh Courts through the decision in R (on the application of Bridges) v Chief Constable of South Wales.[56] This involved an examination of the trial use of automatic facial recognition software. Importantly, the case involved the overt use of such systems and so its findings do not address the issues that may be presented by covert use and compliance with the Regulation of Investigatory Powers Act 200. However, the conclusions of the Court merit detailed consideration and are contained verbatim in **Appendix 3 and are summarised in the box at Section 3.5.2.**

There are a few critical aspects to their findings. Firstly, they made clear that in evaluating whether there had been an interference with an Article 8 right to privacy, and whether that interference was "in accordance with the law" as a basic rule, "the

[55] Scottish Biometrics Commissioner Act 2020, Section 2 & 3.
[56] [2020] 1 W.L.R. 5037

more intrusive the act complained of, the more precise and specific the law must be."[57] Law here is construed broadly to include the policies that accompany legal frameworks. Following on from this, the Court in this case were critical of the governance framework in use by the police force at the time of the pilot. In particular, the Courts expressed that there were two areas of discretion that merited greater control: the selection of those individuals who would be included on watch lists when AFR Locate was being deployed and the locations where AFR Locate might be deployed. Further, despite their being a data impact assessment, that assessment had failed to grasp the risk to the human rights and freedoms of data subject. In addition, in order to comply with the public sector equality duty, the police force should had taken steps to specifically evaluate its potential discriminatory impacts (before, during and after the trial). The fact that the police force failed to evaluate the software it had not 'done all that it reasonable could do' to discharge its duty.[58]

The Bridges decision noted the role of the Surveillance Camera Commissioner, and that this role would specifically cover the use of surveillance cameras in the context of AFR.[59]Of particular note, the Court recognised the value of the Code of Practice issued by the Secretary of State and the guidance produced by the Surveillance Camera Commissioner on the 'Police Use of Automated Facial Recognition Technology with Surveillance Camera Technology' issued in March 2019. However, they were critical of the generic nature of each. They emphasised that of particular concern, was that there was no specific policy addressing the justification for the

[57] [2020] 1 W.L.R. 5037

[58] Bernard Keenan, Automatic facial recognition, and the intensification of police surveillance M.L.R. 2021, 84(4), 886-897

[59] S34 Protection of Freedoms Act 2012.

inclusion of an individual on a watch list and similarly no policy providing a justification of selecting particular locations for the use of AFR.

Since the Bridges decision, the role of the Biometrics Commissioner has been brought together with the Surveillance Camera Commissioner. As a result, one individual is appointed to perform this dual role. However, it is important to note that while the Code of Practice and the role of the Biometric and Surveillance Camera Commissioner's relates to England and Wales, they are influential in the framework of accountability. This will particularly be the case where working across borders will require compliance with the frameworks of England and Wales and those in Scotland.

#### 3.2.3.3: Electronic Surveillance and Monitoring Systems

The use of emerging technology for the purposes of electronic surveillance and monitoring will be subject to the regulatory frameworks set out in, the Regulation of Investigatory Powers (Scotland) Act 2000, the Regulation of Investigatory Powers Act 2000, the Police Act 1997 and the Investigatory Powers Act 2016.[60] Where there is a failure to comply with these systems of regulation there is the potential for there to have been a breach of human rights, most likely Art 8 Right to Private and Family life. In addition, it may impact on the potential for the admissibility of evidence that results from such actions to be challenged (Ross et al, 2020).

[60] The electronic monitoring in the context of penal measures has not been examined here. For the regulation of electronic monitoring in that context see the Management of Offenders (Scotland) Act 2019.

The Regulation of Investigatory Powers (Scotland) Act 2000 sets out the framework for the regulation of surveillance addressing 'directed surveillance' and 'intrusive surveillance' and can be used as one illustration of how the current patchwork of legislation may impact on the lawful use of emerging technology.[61] Surveillance is directed when it is covert surveillance that is not intrusive, relates to a specific investigation or operation, and is likely to result in obtaining private information about a person who may or may not be the focus of an investigation and takes place in circumstances where authorisation is not possible.[62] Intrusive surveillance is covert surveillance that focuses on residential premises or private vehicle where that surveillance is carried out by an individual but also where it is carried out by means of a surveillance device.[63] Importantly, surveillance will not generally be considered intrusive when a surveillance device is not specifically located on the premises/in the vehicle subject to surveillance, but it will be considered intrusive if such remote surveillance technology can achieve a sufficiently reliable quality of data.[64]

Authorisation of directed surveillance can be given in circumstances where the designated person is of the view that the action is necessary and proportionate.[65] The grounds on which authorisation of directed surveillance can be given are much broader than that for which authorisation intrusive surveillance can be given. Directed surveillance can be authorised on the grounds that it is necessary to prevent or detect crime or prevent disorder, in the interests of public safety or for the protection of public health. On the other hand, intrusive surveillance can be

[61] The Regulation of Investigatory Powers (Scotland) Act 2000, Section 1.
[62] The Regulation of Investigatory Powers (Scotland) Act 2000, Section 1(2).
[63] The Regulation of Investigatory Powers (Scotland) Act 2000, Section 1(3).
[64] The Regulation of Investigatory Powers (Scotland) Act 2000, Section 1(5)(b).
[65] The Regulation of Investigatory Powers (Sc) Act 2000, Section 6(2).

authorised where it is considered necessary to prevent or detect serious crime.[66] Directed surveillance and intrusive surveillance must be authorised by the appropriate designated person in order to be lawful.[67]

The implications of these provisions for the use of emerging technologies is that it is clear that in order to be lawful, consideration has to be given the context and purpose for which the technology is being used e.g. covert use, directed surveillance etc. Thereafter, a system of authorisation will need to be embedded to ensure that the technology is accompanied by the appropriate authorisation.[68]

In assessing whether intrusive surveillance was necessary and proportionate consideration will be given to whether the same information could be obtained by other means. What this means in the context of emerging technology is that if a technology is developed that would obtain the same data, as an already available means, consideration should be given to whether the use of that technology is needed at all.

**Regulation of Automated Decision Making**

The Council of Europe Convention for the protection of individual with regards to the processing of personal data sets out the international framework that supports data protection. Applying to both public and private sector, it requires that state parties ensure that data should be processed in a matter that is fair and transparent, does

[66] The Regulation of Investigatory Powers (Scotland) Act 2010. Section 10(2)(a).
[67] The Regulation of Investigatory Powers (Sc) Act 2000, Section 8(1) and Section 10(1A) respectively.
[68] HMA v Purves, 2009 SLT 296.

not go beyond the scope of the original purpose and that it is only preserved in a form that allows identification for the shorted possible period of time.[69] While the Convention does allow the processing of special categories of data such as biometric data, and genetic data, it is only lawful when accompanied by appropriate safeguards.[70] Further, an individual should not be the subject of a solely automated decision making process unless their views have been taken into account.[71] Importantly, there can be an exception to this provision where it is necessary and proportionate for the prevention, investigation and prosecution of criminal offences.[72] These provisions are implemented into the domestic law through the Data Protection Act 2018 s49 and 50.

In 2017 the Council of Europe's Committee of Experts on Internet Intermediaries completed a study into the human rights implications of automated data processing techniques.[73] The key issues they examined where automation, data analysis, and adaptability. They highlight that an examination of human rights implications must consider the relationship between specific algorithm used and the data set to which it is applied.[74] This is because while it is possible for the design of an algorithm to be inherently flawed by design, it is also possible that the data set to which it is applied contains a particular bias that is then replicated/magnified by the algorithm (Završnik,

[69] Council of Europe, Convention 108+ Convention for the protection of individual with regards to the processing of personal data (as amended 18 May 2018). Article 5(4).
[70] Council of Europe, Convention 108+ Convention for the protection of individual with regards to the processing of personal data (as amended 18 May 2018). Article 6. Special categories of data are equivalent to those protected as 'sensitive' in the UK Data Protection Act 2018 s35(8).
[71] Council of Europe, Convention 108+ Convention for the protection of individual with regards to the processing of personal data (as amended 18 May 2018). Article 9(1)(a).
[72] Council of Europe, Convention 108+ Convention for the protection of individual with regards to the processing of personal data (as amended 18 May 2018). Article 11(1).
[73] 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.
[74] 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. p6.

2021). There are further challenges that result from human interrogation and interpretation of the algorithm (Binns, 2022). The expertise of the human user will be highly influential in whether the algorithms use is human rights compliant.

Specifically, concerns have been raised in the context of automated decision making and the use of artificial intelligence (Binns, 2022). At the moment, regulation of this in the UK is very limited. This is for two reasons. In some cases, the data driving the system would not meet the definition of personal data for the purposes of regulation i.e., it does not relate to an identified or identifiable individual. However, if such data is combined with other data to identify an individual then that will become regulated data. In other cases, the way in which the algorithm is applied to the data is opaque. What this means is that even if the data is captured by the data protection provisions, there will be a limited ability to achieve transparency in how that data is processed.

At this point in the UK the Office for Artificial Intelligence have issues Guidelines for the Procurement of AI in Government (2020) and they offer insights into key considerations. In addition, they have issued an Ethics, Transparency and Accountability Framework (2021) which is accompanied by an algorithmic transparency template (December 2021). Importantly, in contract to the Canadian system discussed later on, they are not legally binding.

The Justice and Home Affairs Committee of the House of Lords, in the UK have raised concerns that there is currently not central register of AI technologies.[75] Their view is that this is problematic because this lack of transparency means their uses cannot be interrogated and in turn, they cannot effectively be held accountable. In the context of policing, they argue that there should be a 'duty of candour' on the police to ensure transparency in the use of AI enabled technologies.[76]

Algorithms have the potential to mask human bias in a cloak of objectivity. The have the potential to exacerbate and escalate those biases.[77] The JHAC made clear that there is a significant "issue that there is no minimum scientific or ethical standards that an AI tool must meet before it can be used in the criminal justice sphere."[78] To this end they suggest that the solution is to establish a national body who can engage in the process. Since the time of their report there has been some progress on this front with the Alan Turning Institute leading a project seeking to draft global technical standards.[79]

There are a number of international developments that can be drawn upon to help frame an ethical approach to the use of algorithms. For example, in May 2019 the OECD issues its Principles of Artificial Intelligence.[80] Shortly after, in June of that

[75] Justice and Homes Affairs Committee, Technology rules? The advent of new technologies in the justice system, 1st Report of Session 2021–22, HL Paper 180. March 2022. p3.
[76] Justice and Homes Affairs Committee, Technology rules? The advent of new technologies in the justice system, 1st Report of Session 2021–22, HL Paper 180. March 2022. p4.
[77] Justice and Homes Affairs Committee, Technology rules? The advent of new technologies in the justice system, 1st Report of Session 2021–22, HL Paper 180. March 2022. p4.
[78] Justice and Homes Affairs Committee, Technology rules? The advent of new technologies in the justice system, 1st Report of Session 2021–22, HL Paper 180. March 2022. p4.
[79] UK Government, New UK initiative to shape global standards for Artificial Intelligence - GOV.UK (www.gov.uk), Press Release.
[80] OECD Principles on Artificial Intelligence May 2019: Artificial intelligence - OECD

year the G20 issues its AI Principles and in November 2021 UNESCO adopted a Recommendation on the Ethics of AI.[81] This patchwork is soon to be further embellished by the work of the Council of Europe who are in the process of developing a convention on the use of AI that is due to be completed in 2023.[82]

[81] 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)
[82] Council of Europe's Work in progress (coe.int)

## 3.3: Recommendations from the existing research examining the adoption and use of new emerging technologies in policing for best practice (including in relation to scientific standards and ethical guidelines) in the wider dissemination of these technologies in police practice

### 3.3.1: Electronic Databases

Thirteen of the documents from the research and policy-relevant literature reviewed offer specific recommendations, guidelines, and suggestions drawn from empirical research directly examining police practice for improving the use of electronic databases in policing (Asaro 2019; Aston et al., 2021; Babuta 2017; Babuta and Oswald 2020; Clavell 2018; McKendrick 2019; National Analytics Solutions 2017; Neiva et al., 2022; Neyroud and Disley 2008; Skogan and Hartnett 2005; Sanders and Henderson 2013; Weaver et al., 2021; Williams et al., 2021). Of these twelve focus on the management and use of data and data sharing technologies between third parties. One specifically makes recommendations for the use of social media technologies and data (Williams et al., 2021) and two specifically include recommendations for data pertaining to vulnerable people (Asaro 2019; Brabuta 2017). Only two of the documents reviewed present specific clear, evidence-based recommendations or guidelines for improving the use of community policing applications and data (Aston et al., 2021, Clavell et al., 2018). None of the documents reviewed presented evidence-based recommendations, guidelines, or examples from best practice for improving the use of data pulling platforms, DNA databases or for the use of open space data. This suggests that these represent areas that require further research to ascertain what might work best in disseminating these forms of technology more widely within policing practice.

#### 3.3.1.1: Data Sharing Platforms and Third-Party Data Sharing

Of those that make specific recommendations for improving the use of databases and third-party data sharing platforms, Neiva et al., (2022) also recommends better management of the expectations of all professionals involved in working together with the police in criminal investigations and suggests that greater communication as to the needs of different sector organisations can held to strengthen the interoperability of working with multiple datasets, as well as help with managing data subjects' privacy and human rights. They argue that this is especially important for when dealing with big data. Skogan and Hartnett (2005) use evidence from a study involving the Chicago Police Department's experiences of centralised data warehouses to emphasise that the need for the host organisation to take an active role in clarifying expectations and setting standard.

Neyroud and Disley (2008) recommend strong transparent management and oversight of data sharing technologies with third party organisations is essential for minimising the risk of criticisms as to the legitimacy of police activity, while Sanders and Henderson (2013) draw upon evidence from Canada to emphasise the need for greater material, social and organisational integration to enable effective use of these technologies. McKendrick (2019) recommend clear transparency regarding the handling of data, especially by private companies and clear information and communications as to data access and limitations by third parties.

Weaver et al., (2021) offers a series of recommendations for improving the service connection juncture between police offers and health professionals over the

management of suicide risk for subjects in police custody and argue that a balance needs to be made between risk assessment and communication between parties. They also discuss how an integrated approach can help facilitate evidence-based assessment, as well as inform the development of data collection, management and sharing processes.

Specific guidance for improving the use of these technologies by achieving greater standardisation of practices is provided by the National Analytics Solutions 2017 report. They argue that there is a need for: 1) Rebalancing the roles and responsibilities of the police professionals with other parts of government who have different cultures and practices regarding the collection, storing, processing and use of data, 2) assessments to be undertaken to establish best practice and decision making, 3) greater clarity over the legal obligations on data storage and processing across all parties, including with private sector third parties, 4) greater clarification over consent issues relating to data subjects, 5) a need for clarification regarding the duration of storage. In addition to minimise the risk of harm, they recommend that data risk assessments should be carried out and argue that Data Protection Laws should serve as the minimum standard of consideration (National Analytics Solutions 2017). They also provide an ethical framework for the management of data and data sharing. For this, they acknowledge that there is a need for ethically operated solutions that ensure that the public can trust the technology and that their privacy will not be placed at risk, arguing that the implementation of such a framework should be underpinned by four dimensions of society, fairness, responsibility, and practicality (ibid). However, they also acknowledge that additional research is required to devise and test an ethical standards framework specifically for big data

(ibid). Similarly, Babuta (2017) specifically recommends the standardisation of concepts for entering information into police databases and calls for a standard lexicon across all parties. They also recommend the creation of shared MASH (Multi-Agency Safeguarding Hubs) to be created to allow for better data sharing practices and partner agencies, underpinned by the development of a clear decision-making framework at the national level to ensure ethical storage, management, and use of data (ibid).

#### 3.3.1.2: Social Media Platforms and Data

Only one article includes specific recommendations for improving police practice regarding the use of social media technologies and data (Williams et al., 2021). 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 specifically in the policing of hate crime and malicious social media communications.

#### 3.3.1.3: Vulnerable Population Databases and Datasets

Two documents discuss specific recommendations for vulnerable population databases and datasets (Asaro 2019; Babuta 2017). Asaro (2019) outlines the need for the development and implementation of an Ethics of Care approach to the management and use of data concerning vulnerable data subjects, whereas Babuta (2017) discusses how the management of data concerning vulnerable people is currently conducted in the UK using local police datasets. Babuta (2017) argues that local authorities, social services, and the police should collaborate closely when identifying vulnerable individuals in need of safeguarding and suggest that MASH

databases would help to facilitate this. However, they argue that further research into the use of national datasets is necessary to gain a better understanding of the risks involved in the use of such technologies.

#### 3.3.1.4: Community Policing Applications

Two of the documents presents specific clear, evidence-based recommendations for improving the use of community policing applications and data (Aston et al., 2021; Clavell et al., 2018). Aston et al., (2021) draws on evidence from interviews conducted with members of the public from minority backgrounds and members of organisations who work with minority population groups and police agencies in 9 countries in Europe to argue that community policing models, data protection and security procedures can enhance public confidence in sharing information with the police. Data protection and the potential abuse of information need to be addressed through secure storage of information and it is argued that demonstrating enhanced data security through improvements to data storage systems and protections and procedures can demonstrate a procedurally just approach that will improve public confidence in policing and in information sharing (Aston et al., 2021). Clavell et al., (2018) present a set of ethical guidelines drawn from empirical research to ensure that the use of technology in community policing does not result in increased victimisation, inequalities and inefficiency in its storage and use, and suggests that greater integration between academic researchers and the policy community is needed to develop and implement specific solutions that are sensitive to the needs of all parties (see example 1 on page 80).

### 3.3.2: Biometric Identification Systems

Twenty-one of the documents reviewed offer specific recommendations, guidelines, and suggestions drawn from empirical research examining police practice for the adoption and dissemination of biometric identification systems in policing (Alikhademi et al., 2022; Almeida et al., 2021; Asaro 2019; Babuta 2017; Babuta and Oswald 2017; Bradford et al.,

Example 1: Evidence-Based Recommendations for Best Practice: Implementation of ICT-mediated Community Policing Resources (Clavell et al., 2018)

In order to ensure a successful implementation of ICT-mediated community policing resources, the following aspects need to be taken into account:

1. Relevance

Clear needs, goals and demands have to be detected

2. Empowerment

The preferences of both LEAs and citizenry have to be taken into account.

3. Stakeholders

A wide scope of stakeholders has to be considered

4. Context

It is important to bear in mind the spatial and temporal conditions that will affect the functioning of the system

5. Trust

Transparency and accountability should not be seen as trade-offs or obstacles for an effective policing strategy.

6. Agency and Participation

Differing involvement levels available for citizenry may co-exist. However, undesired or involuntary involvement is strongly discouraged.

7. Safety

The involvement of citizens in security tasks has to be limited. Otherwise, disproportionate risks could be assumed by community members that are not prepared or legally entitled for certain high risk actions or involvements

8. Anonymity

The anonymous interaction through ICTs should not be perceived as a drawback. It could make people more willing to participate and collaborate

9. Social Media

Social media reutilization of other's contents by both LEAs and citizens has to be carried out with precaution

10. Accessibility

Usability and simplicity of functions help to achieve the relevant goals as well as to compensate for the regulation complexity maintenance.

2022; Bragias et al., 2021; Clavell 2018; Dechesne 2019; Ernst et al., 2021; L'Hoiry et al., 2021; McKendrick 2019; National Analytics Solutions 2017; Neyroud and Disley 2008; Oswald 2019; Smith and Miller 2022; Urquhart and Miranda 2021; van 't Wald et al., 2021, Whittelstone 2019; Wilson and Kovac 2021; Williams 2020). Of these eight discuss the management of facial recognition technologies, while 13 propose recommendations and suggestions for the use of artificial intelligence technologies. None of the documents reviewed offer suggestions for voice recognition technologies, suggesting that this is another possible area for future research.

#### 3.3.2.1: Facial Recognition Technologies

Recommendations pertaining to the use of facial recognition technologies focus on improving public support for the use of these technologies as well as the need to devise new ethical principles and guidelines for the use of these forms of technology. For example, Bragias et al. (2021) suggest that if police authorities and policy makers identify and address the specific concerns raised by members of the public and are transparent in their practices and educate the public about misinformation, trust, confidence, and support for the use of FRT by police may increase. Williams (2020) argues that trust in systems like facial recognition technologies and biometric identification systems which are predicated on human prejudicial biases and assumptions would increase if biases and limitations as to the efficiency of these systems were named and interrogated prior to development. Babuta and Oswald (2020) explain that the current lack of organisational guidelines or clear processes for scrutiny, regulation, and enforcement of biometric identification systems, including facial recognition technologies should be addressed as part of a new draft

code of practice. This should specify clear responsibilities for policing bodies regarding scrutiny, regulation, and enforcement of these new standards. Similarly, Smith and Miller (2022) argue that clear, ethical principles and guidance should be implemented in a standardised manner to mediate the potential conflicts in relation to these technologies concerning security on one hand and individual privacy and autonomy on the other They also argue that these principles can be used to support appropriate law and regulation for the technology as it continues to develop. The National Physical Laboratory and Metropolitan Police Force (2020) recommend further trials to be conducted to explore the benefits and limitations of the use of facial recognition technologies in different policing activities and argue that careful consideration must be made using these technologies in defined spaces and that decisions should be carefully made as to where and how these technologies should be deployed. Chowdhury (2020) recommends a generational ban on the use of these technologies until further guidelines and legal stipulations have been developed and argues that mandatory equality impact assessments should be introduced. They also recommend the collection and reporting of ethnicity data and regular, independent audits, as well as the introduction of protections for minority groups.

#### 3.3.2.2: Artificial Intelligence

Recommendations and suggestions from the existing research in relation to Artificial Intelligence technologies focus on three key themes: 1) minimising bias, especially bias towards marginalised communities, 2) establishing standards for predictive policing technologies, and 3) raising awareness via enhancing communications

about algorithms to foster greater understanding of what these forms of technological applications involve.

For example, Alikhademi et al., (2022) discusses the use of Artificial Intelligence in predictive policing and how they can replicate the systemic bias of previous human decision-makers. They recommend that the pros and cons of the technology need to be evaluated holistically to determine whether, how and when these technologies should be used in policing. Similarly, Asaro (2019) argues that the adoption of AI technologies needs to be undertaken alongside educational processes designed to enhance critical understanding of the datasets it operates and the biases that these datasets may represent. From this, they recommend an AI Ethics of Care approach to minimise the risk of harm and improve perceptions of fairness. According to Asaro (2019: 44), an ethics of care approach takes a holistic view of the values and goals of systems designs and considers the interaction and interrelation between an intervention and the predicting of outcomes within specific contexts. The goals and values of the technology and its implementation should be of benefit to everyone (ibid). Whittlestone (2019) argue that high level principles can help to ensure that these technologies are developed in ways in that minimise the risk of bias against marginalised groups. They also recommend building consensus around their use within policing and with other institutions in ways that are culturally and ethically sensitive. They also suggest that the costs and benefits of the use of these technologies for marginalised groups should be weighed up prior to their implementation for specific purposes. In addition, they recommend building on existing public engagement efforts to understand the perspectives of different publics surrounding the use of these technologies, especially those from marginalised

communities to inform decisions making about the implementations of these technologies (Whittletone 2019).

Five of the documents reviewed discuss the need for clear, ethical guidelines and laws to minimise the potential harms associated with the use of artificial intelligence technologies in policing and offer research-informed suggestions to this end (Almeida et al., 2021; Alikhademi et al., 2022; Asaro 2019; Whittelstone 2019; Urquhart and Miranda 2021).For example, Alikhademi et al., (2022) reviews the existing research focusing on the issue of fairness in relation to machine learning and artificial intelligence in predictive policing to develop a set of recommendations for fair predictive policing to minimise the risk of racial bias (see example 2) Whittlestone (2019) recommend the development of a set of shared concepts and terminology to develop an ethics of algorithms and AI and suggest that further research is needed to explore the ambiguity on commonly used terms from which to build consensus for use in ways that are culturally and ethically sensitive. In addition, they also recommend the building of a more rigorous evidence base for the discussion of social and ethical issues surrounding the use of AI in policing. Finally, Hobson et al., (2021) argue that greater awareness and exposure to the successful use of algorithms through trials can help to enhance the general acceptability of these technologies.

### 3.3.3: Surveillance Technologies and Tracking Devices

Fourteen of the documents from the research and policy-relevant literature reviewed offer specific recommendations, guidelines, and suggestions drawn from empirical research directly examining police practice for improving the use of surveillance technologies and tracking device technologies in policing (Aston et al., 2022; Laufs and Borrion 2021; Koper et al., 2019; Hendrix et al., 2019; Lum et al., 2019; White et al., 2018; Gramagila and Phillips 2018; Miranda 2022; Murphy and Estcourt 2020; Todak et al., 2018; Smykla et al., 2016; Brookman and Jones 2020; Clavell et al., 2018; Asaro 2019). Of these two make recommendations for the use of technology in hot spot analysis, 2 provide recommendations for improving the use of CCTV and visual optical technologies, 1 makes recommendations for the design and implementation of autonomous robots, while 7 provide recommendations for the adoption and dissemination of body worn cameras in policing practice. None of the documents reviewed provide recommendations or examples of good practice in the implementation of drones.

Example 2 :Evidenced-Based Recommendations for Best Practice:

Recommendations for Improving Predictive Policing to Minimise Racial Bias (Alikhademi et al., 2021)

1. Pre-processing of data

Datasets should prevent discrimination by reducing the output's dependence on variables that have been identified as discriminatory

2. Algorithm design

Use of counterfactual analysis processes to detect and correct bias

3. Post-processing of data

Use of Lohia's method in the post-processing of the results of an algorithm to make them respect group and individual fairness.

4. Analysis of results

Use of statistical measures to evaluate the fairness of outcomes for groups.

### 3.3.3.1: Location and ‘Hot spot’ Analysis Technologies

Two articles provide recommendations for the use of hot spot location analysis technologies (Koper et al., 2019; Hendrix et al., 2019). Koper et al., (2019) argue that greater training and emphasis on strategic uses of IT for problem-solving and crime prevention, and greater attention to the behavioural effects that these forms of technology may have on officers, might enhance its application for crime reduction. Hendrix et al., (2019) suggest that police institutions should develop a plan for how the use of these forms of technology fit within its operational goals and guiding philosophy to improve the correspondence between the adoption of these technologies and strategic goals.

### 3.3.3.2: Body Worn Cameras

Specific recommendations for improving the implementation of these technologies are made in seven of the documents focusing on the use of body worn cameras in policing (Lum et al., 2019; Gramagila and Phillips 2018; Miranda 2022; Murphy and Estcourt 2020; Todak et al., 2018; White et al., 2018; Smykla et al., 2016). Specific recommendations were made by Lum et al., (2019), who explain that to maximise the positive impacts of BWCs, police and researchers will need to give more attention to the ways and contexts (organizational and community) in which BWCs are most beneficial or harmful and will need to address how BWCs can be used in police training, management, and internal investigations to achieve more fundamental organizational changes with the long-term potential to improve police accountability and legitimacy in the community. White et al., (2018) draw on the findings from research in the US policing context to demonstrate that adherence to

the U.S. DOJ BWC Implementation Guide can lead to high levels of integration and acceptance among key stakeholders. From research in both the US and Australia, Murphy and Estcourt (2020) recommend that the public should be involved in the formulation of police guidelines concerning the use of these technologies in order to democratise the rules around body-worn cameras and reduce controversy regarding their implementation. Todak et al., (2018) drawn on research evidence to reveal how decisions to implement BWCs carry unique consequences for external stakeholders and recommend for a comprehensive planning process that takes into account the views of all stakeholders to be implemented prior to rollout. Finally, Smykla et al. (2016) discusses the impact that the media play on the acceptance of this form of technology and recommend for the potential impacts of BWCs on safety, privacy, and police effectiveness to be assessed prior to deployment.

#### 3.3.3.3: Autonomous Security Robots

One article presents important recommendations and considerations regarding the use of autonomous robotic devices in policing. Asaro (2019) considers the serious challenges in automating violence and suggests that at the very least, strict ethical codes and laws pertaining to the use of these technologies need to be developed. However, given the level of harm that these devices can pose, Asaro (2019) also recommends for these to be banned in police and security practices.

#### 3.3.3.4: CCTV and Visual/Optic Technologies

Four articles offer suggestions for improving the use of CCTV and visual/optic technologies in certain aspects of policing practice (Brookman and Jones 2020; Clavell et al., 2018, Aston et al., 2002; Laufs and Borrion, 2021). Brookman and

Jones (2020) recommend the need to introduce and refine clear standards and principles concerning the use of these technologies in forensic investigations, while Clavell et al., (2018) suggest that the positive and negative external factors at play at the intersection between technology, society and urban management need to be explored to help manage expectations concerning these technologies..

### *3.3.4: Recommendations from Research for Best Practice in the Development and Application of Ethical Frameworks and Scientific Standards in Relation to Emerging Technology*

Ten of the documents reviewed present recommendations drawn from research for the development and application of ethical frameworks and scientific standards in relation to emerging technologies in policing (Almeida et al., 2021; Laufs and Borrion 2021; Aston et al., 2021; Oswald 2019; Ernst et al., 2021; Whittelstone 2019; Strom 2017; Dechesne 2019; Bradford et al., 2022, and Aston et al., 2022). Of these, one draws on research evidence in relation to electronic databases (Aston et al., 2021), seven in relation to biometric identification systems and AI (Almeida et al., 2021; Ernst et al., 2021; Oswald 2019; Whittelstone et al., 2019; Strom 2017; Bradford et al., 2022; Dechesne 2019) and two in relation to surveillance and monitoring technologies (Laufs and Borrion 2021 and Aston et al., 2022).

#### **3.3.4.1: Electronic Databases**

One of the articles (Aston et al., 2021) looks at evidence from research with members of the public in 9 European countries to make recommendations for developing and applying ethical standards in relation to the sharing of data in

community policing applications. They argue that community policing models, data protection and security procedures can help enhance public confidence in relation to information sharing. They argue that demonstrating enhanced data security through improvements to systems, data storage, protection and procedures will help to improve information sharing. None of the documents focus specifically on scientific standards for electronic databases.

#### 3.3.4.2: Biometric Identification Systems and AI

Of the seven documents that draw on evidence from research for the development and application of ethical frameworks and scientific standards in relation to biometric identification technologies and artificial intelligence, six focus on the development and application of ethical standards (Almeida et al., 2021; Oswald et al., 2019; Whittelstone 2019; Strom 2017; Dechesne 2019; Bradford et al. 2017). Three of the documents discuss scientific standards (Ernst et al., 2021; Oswald 2019; Strom 2017).

Of the six that focus on the development and application of ethical frameworks, one uses evidence from research for the development of ethical standards specifically in relation to facial recognition technologies (Almeida et al., 2021) by looking at evidence from the UK, US and EU concerning the use and misuse of facial recognition technologies. From this, they recommend that there needs to be better checks and balances for individuals and societal needs, greater accountability through improved transparency, regulation, audit, and explanation of facial recognition technology use., and the use of data protection impact assessments and human rights assessments. They also pose 10 ethical questions that need to be

considered for the ethical development, procurement, rollout, and use of facial recognition technologies for law enforcement purposes (see example 3).

The other five documents use evidence from research for improving best practice via the development and application of ethical guidelines in relation to artificial intelligence (Strom 2017, Whittelstone et al., 2019; Dechesne 2019; Bradford et al., 2019; Oswald 2019). For example, Whittelstone et al., (2019) explores the applicability of various sets of published prescriptive principles and codes used to guide the development and use of these technologies. For example, they explore the Asilomar AI Principles developed in 2017 which outline guidelines on how research should be conducted and list the ethics and values that AI must respect. They also explore the Partnership on AI which has established a set of criteria for guiding the development and use of AI and which technology companies should uphold. They also discuss the five principles from the House of Lords Select Committee on Artificial Intelligence and the cross-sector AI code, as well as the Global Initiative on Ethics of Automous and Intelligence Systems' set of principles for guiding ethical governance of these technologies. By performing a data frequency analysis, Whittelstone et al., (2019) found that there are substantial overlaps between the different sets of principles revealing agreement regarding that these technologies should be used for the common good and should not harm people's rights or shared values such as fairness, privacy, and autonomy.

Example 3: Ten critical ethical questions that need to be considered for the ethical development, procurement, rollout, and use of Facial Recognition Technologies (Almeida et al., 2021)

1. Who should control the development, purchase, and

testing of FRT systems ensuring the proper management and processes to challenge bias?

2. For what purposes and in what contexts is it acceptable

to use FRT to capture individuals' images?

3. What specific consents, notices and checks and balances should be in place for fairness and transparency for these purposes?

4. On what basis should facial data banks be built and used in relation to which purposes?

5. What specific consents, notices and checks and balances should be in place for fairness and transparency for data bank accrual and use and what should not be allowable in terms of data scraping, etc.?

6. What are the limitations of FRT performance capabilities for different purposes taking into consideration the design context?

7. What accountability should be in place for different usages?

8. How can this accountability be explicitly exercised, explained and audited for a range of stakeholder needs?

9. How are complaint and challenge processes enabled and afforded to all?

10. Can counter-AI initiatives be conducted to challenge and test law enforcement and audit systems?

Oswald (2019) draws on lessons learnt from the UK from the West Midlands data ethics mode to recommend a three-pillar approach to achieving trustworthy and accountable use of AI. Oswald (2019) suggests that lessons can be learned specifically in relation to: i) the contribution to effective accountability in respect of ongoing data analytics projects; ii) the importance of the legal and scientific aspects of the interdisciplinary analysis; and iii) the role of necessity and the human rights

framework in guiding the committee's ethical discussion. Oswald argues that a three-pillar approach could contribute to achieving trustworthy and accountable use of emerging technologies in UK policing via governing 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. However, it is noted that more specific information is required in relation to the application of relevant law to the deployment of emerging technologies. In research focusing on the European context, Dechesne (2019) draws upon evidence from research and lessons learnt from police practice in the Netherlands to develop a set of Recommendations for the Responsible use of AI and to ensure alignment with ethical principles applicable in the Netherlands and EU (see example 4).

**Example 4: Recommendations for the responsible use of AI to ensure alignment with ethical principles in the Netherlands and the EU (Dechesne 2019)**

Recommendation 1: Create an AI review board within the organization and consider appointing an “AI Ombudsperson” to ensure independent critical evaluation of the use of AI within the organization.

Recommendation 2: Update the “Code of Ethics” in the organization to include considerations particularly important for AI scientists and/or develop clear ethics guidelines for AI scientists working in the organization.

Recommendation 3: Support and incentivize the inclusion of ethical, legal and social considerations in AI research projects.

Recommendation 4: Train AI scientists continually to raise awareness about the ethical considerations and keep them up-to-date on the recent developments in AI and insights about their ethical impact.

Recommendation 5: Develop the redress process for a wrong or grievance caused by AI systems (e.g. an official apology, compensation, etc.).

Recommendation 6: Put clear and fair processes in place for assessing accountability and responsibility for the results of an AI system.

Recommendation 7: Install evaluation procedures for the development and use of AI systems that include ethical evaluation

Recommendation 8: Develop auditing mechanisms for AI systems to identify unintended effects such as bias.

Recommendation 9: Develop and deploy AI systems taking into consideration that errors will occur. Assess the error tolerance and acceptability in the envisioned task domain, and put in place measures to prevent, detect and mitigate errors

Recommendation 10: Ensure that used AI systems are sufficiently transparent to enable accountability, usage in courtrooms and the enhancement of trust from the public.

Recommendation 11: Respect the privacy of individuals. Don’t gather more data than needed, store it securely, and realize that anonymization is an imperfect protection.

Recommendation 12: Ensure that users of AI retain a sense of human agency and feel empowered by the system rather than marginalized.

Three of the documents focusing on biometric identification systems and AI draw on research evidence and evidence from police practice to make recommendations for best practice concerning scientific standards for emerging technologies (Strom 2017; Oswald 2019; Ernst et al 2021). All three of these focus on scientific standards for artificial intelligence technologies. Ernst et al., (2021) examines the lessons learned from experimentation with various forms of innovative technology in the Netherlands National police and developed a series of recommendations concerning scientific standards based on the findings. In particular, they discuss how high-end technology requires specific support and facilitating services that need to be provided. They recommend that a strategic vision on technology and innovation should be developed and that support for the technology inside and outside the organisation needs to be implemented. Strom (2017) draws on evidence from research in the US to consider the value of establishing a national technology clearinghouse. They found that there is a need for technological guidance along with strategic guidance for the acquisition of new forms of technology. From this, they argue that a clearinghouse would assist in helping to avoid the purchase of technologies with a high probability of failure.

Oswald (2019) discusses the importance of scientific validity drawing on evidence from the West Midlands context in England to demonstrate the need to consider the statistical and scientific validity of the use of proposed technologies and to the assumptions and values built into the analysis. From this, Oswald (2019) 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. This is because, at present, the development of policing algorithms is often not underpinned by robust empirical evidence regarding their scientific validity. As a result, claims of predictive accuracy are often misjudged or misinterpreted and makes it difficult to assess the actual impact of the technology in practice (ibid). It also explains that the 'Most Serious Violence' predictive model, proposed by the National Data Analytics Solution project had to be withdrawn due to concerns with statistical validity.

Oswald (2019) also discusses how other police forces in the UK have investigate predictive models, including the OxRec model developed by Oxford University, and which was trialled by Thames Valley Police. The OxRec model provides an interface for the calculation of individual risk levels. However, trials have shown that the tool has a low predictive accuracy at the individual level, meaning that it cannot be justified as ethical in terms of avoiding unnecessary harm. Oswald (2019) also recommends that a national ethics approach would require clear scientific standards that are written with the policing context in mind.

#### 3.3.4.3: Surveillance Technologies and Tracking Devices

Two of the documents reviewed drew on evidence from research for recommendations for the development and application of ethical frameworks in relation to surveillance technologies (Aston et al., 2022; Laufs and Borrion 2021). However, neither of these focused specifically on the issue of scientific standards. For example, Laufs and Borrion (2021) drew on evidence from interviews conducted with policing professionals in London and highlighted the current lack of guidelines and evidence with regard to social acceptability. From this, they recommend that

evaluation processes should be formalised and made more inclusive to ensure issues of ethics and social acceptability are not overshadowed by budgetary constraints and resource shortage.

Table 2 presents a summary of the findings of the recommendations for best practice for each type of technology.

| Table 2 - Summary of Findings: Recommendations for Best Practice for Implementation and Dissemination of Emerging Technologies | | |
|---|---|---|
| **Technology Type** | **Specific Technology** | **Recommendations** |
| Electronic Databases | Data Sharing Platforms and Third-Party Data Sharing | • Improved Organisational Integration between Parties |
| | | • Greater Standardisation of Practice |
| | | • Assessment of Best Practice |
| | | • Clarity over Legal Obligations on Data Storage and Processing |
| | | • Implementation of Risk Assessments |
| | | • Use of Ethical Frameworks (inc. specifically for Big Data) |
| | | • Creation of a Multi-Agency Safeguarding Hub |
| | Social Media Platforms | • Greater Cooperation between Policy, Social Science and Technology Researchers in Ethical Guidelines Development |
| | Vulnerable Population Databases and Datasets | • Implementation of an Ethics of Care Approach |
| | | • Greater collaboration between Parties when Identifying Vulnerable Individuals |
| | Community Policing Apps | • Application of Community Policing Models, Data Protection and Security Procedures |
| | | • Implementation of Evidence-Based Ethical Guidelines |
| Biomedical Identification Systems | Facial Recognition Technologies | • Transparency over Biases and Limitations in Efficiency |
| | | • Organisational Guidelines and Codes of Practice with Clearly Outlined Responsibilities |
| | | • Standardisation of Implementation of Ethical Principles |
| | | • Audits on the Collection and Reporting of Ethnicity Data |
| | Artificial Intelligence | • Holistic Evaluation to Determine When and How these Technologies Should be Applied |
| | | • Education to Enhance Critical Understanding of Inherent Biases |
| | | • Implementation of an AI Ethics of Care Approach |
| | | • Evaluation of Costs and Benefits for Marginalised Groups Prior to Implementation |

| | | |
|---|---|---|
| | | • Development of Shared Concepts and Terminology for Development of An Ethics of Algorithms |
| | | • Development of Ethical Frameworks that include Use of Data Protection Impact Assessments and Human Rights Assessments |
| | | • Consideration of Almedia et al.'s (2021) 10 Ethical Questions |
| | | • Application of Dechesne's (2019) Recommendations to Ensure Alignment with Ethical Principles |
| | | • Specific Guidance for the Acquisition of New Technologies |
| | | • Establishment of a National Technology Clearinghouse |
| | | • Evaluation of Statistical Algorithms |
| Surveillance Technologies and Tracking Devices | Location and Hot Spot Analysis Technologies | • Attention to be Given to the Behavioural Effects of these Technologies |
| | Body Worn Cameras | • Use of Technologies to Align with Strategic Goals |
| | | • Development and Adherence to Implementation Guidelines |
| | | • Comprehensive Planning Processes that Consider the Views of all Stakeholders |
| | Autonomous Security Robots | • Development of Strict Ethical Codes and Laws |
| | CCTV & Visual/Optical Technologies | • Clear Standards and Principles Regarding the Use of Technology in Forensic Investigation |
| | | • Consideration of External Social Factors to Manage Expectations |
| | | • Formalised Evaluation Processes |

## 3.4: Recommendations and Lessons Learnt from Research and from the Trials, Adoption and Dissemination of Similar Types of Emerging Technologies in the Health and Children and Family Sectors

The findings from the supplementary review of the academic concerning the use of emergent technologies (electronic databases, biometric information systems and Artificial Intelligence systems, and electronic surveillance and tracking technologies) within the Health Care sector and the Children and Families sector offer a number of recommendations that might be helpful for informing best practice in the implementation and dissemination number of these technologies in policing.

### 3.4.1: Electronic Databases

Four of the 26 articles within this sample provide valuable lessons and recommendations that may be used to help influence the adoption and dissemination of emerging electronic database technologies in policing in ways that may help to prevent potential problems from occurring.

Facca et al., (2020) examined the ethical issues associated with digital data and its use in relation to minors within the health sector. The issues that emerged concerned consent, data handling, minors' data rights, private versus public conceptualizations of data generated
through social media, and gatekeeping. Furthermore, they suggest that the uncertainty concerning the ethics involving minors and digital technology may lead to preclusion of minors from otherwise important lines of research inquiry and that restricting this raises its own ethical challenges. From this, they recommend greater

integrated (cross sectoral) discussion to co-produce guidelines or standards concerning ethical practice between researchers and minors as a mechanism to proceed with such research while addressing concerns around uncertainty. Although this research concerns the health sector, it raises an important issue worthy of consideration for the implementation of emerging technologies within policing – that of considering the use of electronic databases and data in relation to minors.

A study conducted by Schwarz et al., (2021) explored the effects of sharing electronic health records with people affected by mental health conditions and highlighted several ethical and practical challenges that require further exploration. They found that access to information about themselves was associated with empowerment and helped increase patient trust in health professionals. However, negative experiences resulted from inaccurate notes, disrespectful language use, or the uncovering of undiscussed diagnoses. From this, they recommended the development of guidelines and trainings to better prepare both service users and professionals on how to write and read notes. This can be regarded as an important consideration for the implementation of emerging technologies in policing as standards will need to be set regarding subject access to records held about them. In addition, it provides a cautionary tale about the types of language and content to be avoided when entering data and highlights the need for guidance to be provided for those entering data and for those accessing the data in order to prevent harm. Similarly, Sleigh and Vavena (2021) discuss the ethics concerning the collection, sharing, and analysing of personal data in biomedical settings and highlight the need for proactive public engagement to enhance transparency to build public trust, which again provides an important consideration for the use of electronic data in policing

practice. Finally, Birchley et al., (2017) study of the ethical issues involved in developing smart-home health technologies provides some important considerations that may be transferable to the policing context. They describe how one of the key concerns arose over the privacy of the data held, as well as its use, which manifested in emotive concerns about being monitored, arguing that the provision of clear information about the sharing of data with third parties can help to remedy concerns.

### 3.4.2: Biometric Identification Systems and Artificial Intelligence

While none of the documents from the supplementary systematic review offered suggestions that may be helpful for the implementation of facial or voice recognition technologies, a small number offered potentially transferable suggestions from the rollout of artificial intelligence technologies (5 out of 26 documents).

For example, Aicardi et al., (2018) provides a practice-based, self-reflexive assessment of the use of AI in health research to guide policy makers and communities who engage with these technologies and these issues. Similarly, Blease et al., (2019) examine the use of AI in UK General Practitioner Health Care to help assess the potential impact of future technology on key tasks in primary care to pre-empt likely social and ethical concerns, which they recommend should be carried out with professionals working in fields that are seeking to adopt these technologies. Ronquillo et al., (2021) developed a consensus paper on the central points of an international invitational think-tank on nursing and artificial intelligence (AI) and identified priorities for action, opportunities, and recommendations to address existing concerns and challenges. The specific challenges they identified as priorities

for consideration were that: (a) professionals need to understand the relationship between the data they collect and AI technologies they use; (b) they must be meaningfully involved in all stages of AI: from development to implementation; and (c) limitations in the knowledge regarding the potential for professionals to contribute to the development of AI technologies should be addressed. They argue that the nursing profession should be more involved in the conversations surrounding AI given the significant impact that it will have on nursing practice and suggest that action must be undertaken to ensure that professionals understand the relationship between the data they collect and AI technologies they use. These present important lessons and considerations for thinking about when planning the implementation and dissemination of emerging technologies in police practice.

### 3.4.3: Surveillance Technologies and Tracking Devices

Two articles from the supplementary search and review process offer lessons and recommendations from research and practice in the Health and Children and Families' sectors concerning the use of these technologies that are worthy of consideration for informing the implementation of this type of technology in policing practice (Birchley et al., 2017; Zhu et al., 2021). However, these only concern the use of smart devices and sensors, with none of the documents reviewed during this part of the research process offering suggestions specifically for the other types of surveillance technologies discussed in this report. Birchley et al., (2017) reveal that public concerns around the use of these devices in health care settings revolve mostly around the issue of privacy and suggest greater consideration needs to be made with regard to the issue of privacy in the implementation of these technologies. Zhu et al., (2021) also explore the issues concerning privacy and security and argue

that professionals should be involved in the design and implementation of these technologies to help promote ethical awareness and practice.

### 3.4.4: The Use of Research Evidence for Best Practice in the Health and Children and Families Sectors in the Development and Application of Ethical Frameworks and Scientific Standards: Considerations for Policing

Two of the documents reviewed present suggestions from research in the health and children and families sectors (and general public sector) that may be helpful for taking into consideration when thinking about the development and application of ethical frameworks and scientific standards for policing (Leslie 2019; Fukuda-Parr and Gibbons (2021). Both these documents discuss these issues specifically in relation to artificial intelligence. For example, Fukuda-Parr and Gibbons (2021) discuss how voluntary guidelines on ethical practices issued by governments and other professional organisations attempt to create a consensus on core standards and principles for ethical design, development, and deployment of artificial intelligence. However, these ethical frameworks can be regarded as weak in terms of standards for accountability, enforceability, and participation, and for their potential to address inequalities and discrimination (ibid). It is argued that this therefore exposes a need for governments to develop more rigorous standards grounded in international human rights frameworks that are capable for holding Big Tech to account. From this, the authors recommend that AI guidelines should be honest about their potential for widening 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 applications. Leslie (2019) provides an ethical platform for the responsible delivery of an AI project or trial in the public sector context that may be helpful for considering in relation to policing (see example 5).

**Table 3** provides a summary of the recommendations from this body of literature focusing on the use of emerging technologies in other institutions that are transferrable to the policing context.

Example 5: Critical Components of an Ethically Permissible AI Project

(Leslie 2019)

Considerations for AI Projects and Trials in Policing

An AI technology project can be considered to be ethically permissible by considering the impacts it may have on the wellbeing of affected stakeholders and communities and demonstrating:

The project is fair and non-discriminatory

This can be achieved by accounting for its potential to have discriminatory effects on individuals and social groups, by mitigating biases that may influence your model's outputs, and by being aware of the issues surrounding fairness that come into play at every phase of the design and implementation pipeline.

The project is worthy of public trust

For this to be achieved, the safety, accuracy, reliability, security and robustness of its product must be guaranteed to the maximum possible extent

The project is justifiable

This requires prioritisation of the transparency of the process by which the model is designed and implemented, and the transparency and interpretability of its decisions and behaviours.

**Table 3**

**Summary of Findings: Recommendations for Best Practice for Policing from the Literature Focusing on Emerging Technologies in Other Public Sector Organisations**

| Technology Type | Recommendations |
|---|---|
| Electronic Databases | • Greater Integrated Discussion between Professionals involved in Cross-Sectoral Working to Co-Produce Guidelines and Standards Concerning Ethical Practice between Researchers, Professional Institution Personnel and Minors |
| | • Guidelines for Storing and Sharing Data about Minors |
| | • Guidelines for Storing and Sharing Data concerning Mental Health |
| | • Use of Shared Language for Data Input Processes |
| | • Ethical Standards Concerning the Collection, Storing and Sharing of Biomedical Data (e.g., DNA) |
| Biomedical Identification Systems | • Use of Practice-Based Self-Reflexive Assessments |
| | • Education and Training for Professionals |
| Surveillance Technologies and Tracking Devices | • Consideration of Privacy Issues |
| | • Involvement of Professionals in the Design and Implementation Process (those who will be using the technology) |
| | • Government Development of Rigorous Ethical Frameworks Ground upon International Human Rights Frameworks |
| | • Transparency over the Potential Risk of Widening Socio-Economic and Racial Inequalities |
| | • Implementation of Leslie's (2019) Ethical Considerations for AI Research and Trials |

### 3.5: Recommendations from the Analysis of Existing Legal Frameworks Concerning Emerging Technologies

The findings from the analysis of the existing legal frameworks also provides some important insights that need to be considered for the adoption and dissemination of emerging technologies in policing.

In particular, there are lessons that can be learned through an examination of the Information Commissioner's enforcement actions as well as the common law. At this point in time, the ICO has taken a number of steps to raise concerns in relation to technological advances and how they relate to the lawful use of personal information in different public sector contexts.

In June 2021, the ICO issued their investigative report into mobile phone data extraction by Police Scotland. Concerns had been raised about the roll out of cyber kiosks, the collection of data and data analysis in Digital Forensic Hubs.[83] Cyber kiosks was a project established to allow devices to be used by a suitably trained operator, to access a range of digital devices, seeking to consider whether those devices contained material of evidential value. However, the cyber kiosk would not allow any of that data to be extracted or retained. Instead, such processes would have to be carried out by a Digital Forensic Hubs, which have the capacity to extract data. The roll out of cyber kiosks was met with resistance by a range of stakeholders such as civil society groups and the Justice Sub-Committee of the Scottish Parliament.[84]

Concerns primarily involved the lawful basis for processing and the transparency of the information provided to the public about that processing. While acknowledging that progress had been made over the course of the project's development and implementation, the ICO made a number of recommendations that would ensure

[83] 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].
[84] 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]. Para 2.1.1.

future projects of a similar nature would be better placed to comply with data protection law. Those recommendations are contained in the box below.

**ICO Report: Mobile Phone Data Extraction, June 2021**

Recommendation 1:

Police Scotland, the COPFS and the SPA should jointly assess and clarify their mutual relationships and respective roles under the Data Protection Act 2018 in relation to law enforcement processing associated with criminal investigation. They should use the findings of this assessment as the basis for the review and revision of the governance and relevant policy documentation around MPE.

Recommendation 2:

Police Scotland should ensure it has DPIAs in place that cover all of its MPE operations, in order to demonstrate it understands and appropriately addresses the information risks associated with this practice. Police Scotland should review and update such assessments prior to the procurement or roll-out of new hardware or software for MPE and processing, including any analytical capabilities. Where it identifies residual high risks associated with new processing, the force should undertake prior consultation with the ICO, as required under s65 of the DPA 2018.

Recommendation 3:

In order to provide assurance around the integrity of the data extraction processes, Police Scotland should accelerate its work to implement and maintain the standards set out in the Forensic Science Regulator's codes of practice and conduct for forensic science providers and practitioners in the criminal justice system.

Recommendation 4:

Police Scotland should review and revise the information it provides to the public, including the range of documentation it publishes on its website and anything it provides directly to people during engagement. It should ensure that the documentation:

- adequately covers all processing arising from MPE;
- is consistent; and
- provides unambiguous information on privacy and information rights.

When considering this recommendation, the force should engage with, and may wish to adapt to its circumstances, the work the National Police Chiefs' Council Executive (NPCC) is undertaking in relation to digital processing notices as a response to recommendation 2 of the England and Wales report.

Recommendation 5: Police Scotland should review its data retention policy documentation and supplement it with materials to include:

- alignment of regular review and deletion processes across all operational, analytical and forensic environments; and
- processes to allow the separation and deletion of non-relevant material at the earliest opportunity, so that the force does not process it further and so officers cannot inappropriately access, review or disseminate the data.

Recommendation 6:

As far as legislative differences and devolved administration factors allow, Police Scotland should engage with work the UK Government, the NPCC and the College of Policing are undertaking. This work includes: • the statutory power and code of practice being introduced through the Police, Crime, Sentencing and Courts Bill; • police guidance on the considerations and processes involved in MPE; and • privacy information officers provide to people whose devices are taken for examination.

In February 2022, the Information Commissioner's Office issued a reprimand to the Scottish Government and NHS National Services Scotland in relation to the NHS Scotland Covid Status App (Box 2 below). The aim of the app was to enable individuals to prove that they had received the vaccination in order that they could access services (where restrictions applied to unvaccinated individuals). This inevitably involved dealing with sensitive personal information relating to an individual's health. The period of development, evaluation, and roll out were materially affected by the circumstances of the pandemic. The ICO had issued guidance during this period which detailed the key data protection expectations in developing such certification systems. However, the Scottish Government and the NHS National Health Services Scotland, did not appear to have taken on board that guidance. The ICO raised a number of concerns during the apps development and roll out.

**ICO Reprimand: COVID Status App**

Concerns were raised over:

- 3rd party access to retain images provided by user (for verification purposes) to train proprietary facial recognition algorithms (Withdrawn prior to launch).
- Misleading statements on the lawful basis of processing data (Article 5(1)(a) GDPR)
- Lack of appropriate privacy notice (Article 12 & 13 GDPR)
- Failure to comply with the transparency principle (Article 5(1)(a) GDPR)

Reprimand issued in respect of:

- Processing personal data, including sensitive data, in a manner that is unfair in breach of Article 5(1)(a) GDPR
- Failing to provide clear information about the processing of personal data in breach of Article 12 GDPR

In both cases we can draw together the lessons that can be learned. It is critical to:

1. Map the relationship between those involved in the development and implementation of emerging technologies. This is critical to being able to determine roles and responsibilities in the protection of personal information. This is of particular significance when data is being shared between organisations and that data is transferred from the private sector to the public sector or vice versa.
2. Understand the nature of the data that is being processed and the scope of that processing. This will have a knock-on effect on the lawful basis of processing, the need for consent and in turn, the information that needs to be provided to the data subject. For example, if data is collected on the lawful basis that it is necessary for the performance of a specific task relating to the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties there would be an issue if that data is used to train a commercial algorithm, where consent should then be the lawful basis.
3. Undertake a comprehensive review of the above considerations before the deployment of technologies.

Beyond the UK, there is an established relationship of law enforcement and judicial cooperation with the EU.[85] Central to this relationship is the protection of personal data.[86] It is worth noting that while the UK is no longer bound by the Charter of

[85] Trade and Cooperation Agreement between the European Union and the European Atomic Energy Community, of the one part, and the United Kingdom of Great Britain and Northern Ireland, of the other part [2021] OJ L149/10

[86] Article 525, Trade and Cooperation Agreement between the European Union and the European Atomic Energy Community, of the one part, and the United Kingdom of Great Britain and Northern Ireland, of the other part [2021] OJ L149/10

Fundamental Rights, in the context of cross border cooperation, the Union and its member states continue to be bound.[87] The significance of this here is that there may be developments in the scope of the Article 8 Protection of Personal Data that will impact on if, and how, cross border cooperation takes place and in turn introduce compatibility issues in the operationalisation of emerging technologies that are dependent on the processing of personal data. For this reason, when considering the deployment of technologies in a context with high potential for a cross border dimension, compliance with the EU interpretation of Article 8 should be considered.

### 3.5.1: Electronic Databases

The existing case law offers guidance on various criteria that should be applied and factors that will be influential in determining compliance with data protection law and article 8. In many of these cases the key features of compliant use of databases are that they have appropriate policies in place that offer clarity on the circumstances in which data will be retained and the purposes for which it is used.[88] Conversely, those who have non-compliant databases demonstrate confusion over the roles and responsibilities of those processing data and a lack of appropriate governance to ensure compliance. For example, R (on the application of Catt) v Association of Chief Police Officers of England, Wales and Northern Ireland the Court made clear that "the rules in question did not need to be statutory, provided that they operated within a framework of law and that there were effective means of enforcing them".[89]

[87] Article 524, Trade and Cooperation Agreement between the European Union and the European Atomic Energy Community, of the one part, and the United Kingdom of Great Britain and Northern Ireland, of the other part [2021] OJ L149/10

[88] AS1's (A Child) Application for Judicial Review, Re [2021] NIQB 11

[89] R (on the application of Catt) v Association of Chief Police Officers of England, Wales and Northern Ireland [2015] UKSC 9. Also see, R (on the application of M) v The Chief Constable of Sussex Police, Brighton & Hove [2021] EWCA Civ 42.

3.5.2: Biometric Identification Systems

The trial use of automated facial recognition software was subject to detailed examination in the decision of R (on the application of Bridges) v Chief Constable of South Wales and the conclusions of the Court contain important considerations.[90] The Bridges decision provides important guidance that can be used to inform the development of policies and procedures in this area. It set out the following key considerations:

**Key Guidance on the Use of Automated Facial Recognition Software in the UK**

- The more intrusive the act, the more precise and specific the law must be to justify it.
- Data concerned is 'sensitive personal data' within the meaning of the DPA 2018
- Data is processed in an automated way (and demands additional protection)
- Policy required to limit the selection of individuals who would be included in 'watch lists' used by AFR
- Policy required limit the selection of locations for deployment.
- Public Authorities have a positive duty to take reasonable steps to make enquiries about the potential impact of AFR (across the protected characteristics) – to satisfy their equality duty (s149 Equality Act 2010):
  - o These steps should include a before trial, during trial and after trial phase
  - o Assessment of impacts should include a mechanism of independent verification

See: *R (on the application of Bridges) v Chief Constable of South Wales* [2020] EWCA Civ 1058)

[90] [2020] EWCA Civ 1058.

However, it has become apparent that a critical feature of the development and use of biometric systems is the interactions between private entities and law enforcement. This was brought into sharp focus by the role out of Clearview AI's facial recognition tool.

#### 3.5.2.1: Clearview AI: A Comparative View

Clearview AI Inc provide a facial recognition tool that has been deployed by a number of police forces across the globe to conduct retrospective identification.[91] The tool functions by carrying out four consecutive steps:

1. **"scrapes" images** of faces and associated data from publicly accessible online sources (including social media), and stores that information in its database.
2. **creates biometric identifiers** in the form of numerical representations for each image.
3. **allows users to upload an image**, which is then assessed against those biometric identifiers and matched to images in its database; and
4. **provides a list of results**, containing all matching images and metadata. If a user clicks on any of these results, they are directed to the original source page of the image.

However, the use of this tool has been challenged in several jurisdictions. This table sets out the issues raised in Canada, Australia, and the UK.

[91] Live facial recognition presents different concerns. See Information Commissioner's Opinion, The use of live facial recognition technology in public places, 18 June 2021.

| Comparative Regulation of Facial Recognition: Clearview AI Inc | | | |
|---|---|---|---|
| | **Canada**[92] | **Australia**[93] | **UK**[94] |
| General Concerns | 1. False, or misapplied matches could result in reputational damage including becoming a person of interest to law enforcement.<br><br>2. Affront to individuals' privacy rights and broad-based harm inflicted on all members of society, who find themselves under continual mass surveillance by Clearview based on its indiscriminate scraping and processing of their facial images | 1. False, or misapplied matches could result in reputational damage including becoming a person of interest to law enforcement.<br><br>2. Affront to individuals' privacy rights and broad-based harm inflicted on all members of society, who find themselves under continual mass surveillance by Clearview based on its indiscriminate scraping and processing of their facial images<br><br>3. Concerns in relation to the | 1. Continued expansion of the database to include more UK citizens.<br>2. Processing is unfair because individuals are unaware that their personal data is being processed.<br>3. While initial statements were made about the scope of use being limited to law enforcement it has become apparent that they have offered their services to the Government of the Ukraine. This illustrates concerns as to the expansion of the service |

[92] 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.
[93] Office of the Australian Information Commissioner, Commissioner Initiated Investigation into Clearview AI Inc. (Privacy) [2021] AICmr54 (14 October 2021).
[94] ICO issues provisional view to fine Clearview AI Inc over £17 million | ICO [Accessed 18 April 2022].

| | | | |
|---|---|---|---|
| | 3. Concerns in relation to the inclusion of images of children (and other vulnerable individuals). | inclusion of images of children (and other vulnerable individuals). | presenting escalated risks. |
| Grounds of specific legal challenges | 1. Failure to obtain the required consent[95]<br><br>2. Collection, use, and disclosure of personal information was neither appropriate or legitimate[96]<br><br>3. Failure to report the creation of a biometric database.[97] | 1. Failed to obtain the required consent.[98]<br><br>2. Failed to take reasonable steps to implement practices, procedures and systems relating to the entities functions and activities that ensures compliance with the Australian Privacy Principles.[99]<br><br>3. Failed to collect information by lawful and fair means.[100]<br><br>4. Failed to take steps to notify personal of the collection of information.[101] | 1. Failed to process the information of people in the UK in a way they are likely to expect or that is fair;<br>2. Failed to have a process in place to stop the data being retained indefinitely;<br>3. Failed to have a lawful reason for collecting the information;<br>4. Failing to meet the higher data protection standards required for biometric data (classed as 'special category data' under the GDPR and UK GDPR);<br>5. Failed to inform people in the UK about what is |

[95] Clearview contravened: principle 4.3 of Schedule 1, as well as section 6.1 of PIPEDA; section 7(1) of PIPA AB; sections 6-8 of PIPA BC; sections 6 and 12-14 of Quebec's Private Sector Act and sections 44 and 45 of the LCCJTI.

[96] Assessment of appropriateness was carried out applying s5(3) of the Office of the Privacy Commissioner's Guidance on inappropriate data practices.

[97] In violation of sections 45 of the LCCJTI.

[98] Breaching principle 3.3 and 3.4, Schedule 1, Privacy Act 1988.

[99] Breaching 6A Privacy Act 1988.

[100] Breaching principle 3.5, Schedule 1, Privacy Act 1988.

[101] Breaching principle 5, Schedule 1, Privacy Act 1988.

| | | | |
|---|---|---|---|
| | | 5. Failed to take steps to ensure information it used or disclosed was accurate, up-to-date, and relevant. [102] | happening to their data; and<br>6. Asked for additional personal information, including photos, which may have acted as a disincentive to individuals who wish to object to their data being processed.[103] |

The objections raised in the investigation into Clearview's facial recognition tool did not expressly address the legality of the law enforcement use of the tool. However, the critical issue was that the foundation of the lawful collection of data was missing because Clearview scraped data in violation of various websites terms and conditions and did not obtain express consent for images to be used in the creation of the biometric database. This lack of a lawful basis is likely to impact on the legality of sharing this data with law enforcement and the lawfulness of their use of it.

Within the Canadian investigation they were keen to emphasis the potential discriminatory impact of facial recognition technologies, recognising that biometric

[102] Beaching Principle 10.2, Schedule 1, Privacy Act 1988.

[103] Since the time under examination by the ICO straddled before Brexit and after Brexit, infringements were assessed in relation to the GDPR and the UK GDPR. Infringements were found to have occurred in relation to the data protection principles set out in Article 5(1)(a) and Article 5(1)(e) GDPR and UK GDPR; (ii) the requirements of Article 6 GDPR and UK GDPR as to the lawful basis for the processing of personal data; (iii) the requirements of Article 9 GDPR and UK GDPR as to the processing of special category personal data; (iv) the requirements of Article 14 GDPR and UK GDPR as to the information that is to be provided by controllers to data subjects; (v) the requirement of Articles 15, 16, 17, 21 and 22 GDPR and UK GDPR in relation to the rights of data subjects; and (vi) the duty to carry out a Data Protection Impact Assessment under Article 35 GDPR and UK GDPR.

data “is distinctive, unlikely to vary over time, difficult to change and largely unique to the individual.” Research by the National Institute of Standards and Technology was used to support this discussion as it demonstrated that the rate of false positives for Asian and Black individuals was often greater than that for Caucasians, by a factor of 10 to 100 times.[104]

Importantly, it was acknowledged that “facial biometric data is particularly sensitive given that it is a key to an individual’s identity, supporting the ability to identify and surveil individuals.”[105] With a similar concern raised in the New Zealand, Lynch and Chen highlight that FRT differs from other biometrics such as DNA and fingerprints because a person’s face is generally public, and its image can be collected without their knowledge.[106]

Focusing on the risk of harm, the OPC argued that Clearview’s system has the potential to result in misidentification leading to inappropriate police investigations.

In Australia and the UK, they have been criticised as well.[107] The Office of the Australian Information Commissioner and the UK Information Commissioner’s Office

[104] “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.

[105] 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. Issue 2, para 7.

[106] Nessa Lynch and Andrew Chen, Facial Recognition Technology: Considerations for use in policing, December 2021. Available: Facial recognition technology | Police use of emergent technologies | New Zealand Police accessed 16 April 2022. p13.

[107] Office of the Australian Information Commissioner, Commissioner Initiated Investigation into Clearview AI, Inc (Privacy) [2021] AICmr54 (14 October 2021).

conducted their investigation jointly. The OAIC focused on compliance with the Privacy Act 1988 and the ICO focused on compliance with the Data Protection Act 2018 and the EU General Data Protection Regulation.

They acknowledged that the right to privacy was not as absolute right, but rather that an interference could be justified where the processing was necessary, legitimate, and proportionate. However, despite the declared use being for Law Enforcement purposes, the reality of their use went considerably further. Specific issue was taken with the fact that Clearview was a commercial enterprise and was obtaining a commercial advantage through the information's use. In particular, the personal information was used to 'train and improve [Clearview AI Inc's] algorithm and monetize their technology' and the data that they held.[108] In addition, the OAIC was concerned that as a whole the covert way in which Clearview conducted their collection and use of images meant that even if they were to comply in a technical sense with the production of privacy notices – it would be relatively meaningless because affected individuals would most likely not be aware of their practices and in turn do not know to look for the privacy notice.

In the UK ICO had initially announced an intention to fine Clearview AI £17 million. However, the ICO have now issued and enforcement notice and monetary fine of £7,552,800.[109] This fine took into consideration a number of factors that were considered to have mitigated the scope of harm to UK citizens. In particular, Clearview stopped offering their services in the UK. However, the ICO were critical of

[108] Office of the Australian Information Commissioner, Commissioner Initiated Investigation into Clearview AI, Inc (Privacy) [2021] AICmr54 (14 October 2021). Para 178.
[109] ICO Monetary Penalty Notice: Clearview AI Inc Monetary Penalty Notice (ico.org.uk)

the fact that no steps had been taken to exclude the data of UK citizens from matches (conducted elsewhere) or to delete UK citizens data (except in relation to limited direct request for deletion). As a result, accompanying the money penalty, the ICO enforcement notice also requires that specific steps are taken by Clearview to protect the citizens of the UK. Those steps are listed in the box below.

**Steps Required to be Taken by Clearview AI to comply with the ICO Enforcement Notice**

1. Within six months following the date of the expiry of the appeal period, delete any personal data of data subjects resident in the UK that is held in the Clearview Database. Without prejudice to the generality of this requirement, Clearview are to delete any images of UK residents that are held in their database, and any other data associated with such images (including URLs and metadata).
2. Within three months following the date of the expiry of the appeal period, refrain from any further processing of the personal data of data subjects resident in the UK. Without prejudice to the generality of this requirement, Clearview must:

(a) Cease obtained or "scraping" any personal data about UK residents from the public facing internet;

(b) Refrain from adding personal data about UK residents to the Clearview Database; and

(c) Refrain from processing any Probe Images of UK residents, and in particular refrain from seeking to match such images against the Clearview Database.

3. Refrain from offering any service provided by way of the Clearview Database to any customer in the UK.
4. Not do anything in future that would come within paragraphs 1-3 above without first:

(a) carrying out a DPIA compliant with Article 35 35 UK GDPR, and

(b) providing a copy of that DPIA to the Commissioner

### 3.5.2.2: Good Practice in Facial Recognition

The introduction of Clearview AI Incs facial recognition tool has in many ways allowed there to be a meaningfully discussion of the potential impact of the collection and use of biometric data as well as the incorporation of automated decision making

and artificial intelligence. Of particular concern in each jurisdiction has been recognition that although declaring an intention to support Law Enforcement in the prevention and investigation of crime, the reality was that it was a commercial entity collecting, using, and sharing information that was then subsequently being used for Law Enforcement purposes.

Those engaging in policing need to consider if, when, and how emerging technologies are positioned within the regulatory regimes applying to private actors and those applying to public actors (specifically Law Enforcement). This is important because, as the Council of Europe makes clear, such public/private relationships have the potential to blur roles and responsibilities leading to human rights violations.[110]

In 2020, the Council of Europe issued Guidelines on addressing the human rights impacts of algorithmic systems.[111] They propose that before investing in the development of algorithmic systems, states should ensure there will be in place "effective monitoring, assessment, review processes and redress for ensuing adverse effects or, where necessary, abandonment of processes that fail to meet human rights standards."[112]Within those guidelines ""algorithmic systems" are understood as applications that, often using mathematical optimisation techniques, perform one or more tasks such as gathering, combining, cleaning, sorting,

[110] Recommendation CM/Rec(2020)1 of the Committee of Ministers to member States on the human rights impacts of algorithmic systems. Appendix. Para 12.
[111] Recommendation CM/Rec(2020)1 of the Committee of Ministers to member States on the human rights impacts of algorithmic systems. Appendix.
[112] Recommendation CM/Rec(2020)1 of the Committee of Ministers to member States on the human rights impacts of algorithmic systems. Appendix. Para 15.

classifying and inferring data, as well as selection, prioritisation, the making of recommendations and decision making."[113] Accordingly, the applicability of the guidelines is wide ranging and includes for example, facial recognition.

Significantly, the guidelines make clear that consideration should be given to the impact on human rights at every stage from proposal of an algorithm to is operationalisation.[114] Later in 2021 they produced specific guidelines on the use of facial recognition.[115] The virtual of these guidance lines is that they address public and private sector dimension as well as live and retroactive use. They make clear that ultimately "the necessity of the use of facial recognition technologies has to be assessed together with the proportionality to the purpose and the impact on the rights of the data subjects."[116]

Importantly, they highlight that the legal framework should be in place that addresses each type of use and provides "a detailed explanation of the specific use and the purpose; - the minimum reliability and accuracy of the algorithm used; - the retention duration of the photos used; - the possibility of auditing these criteria; - the traceability of the process; - the safeguards". [117] We are to some extent driving in the

[113] Recommendation CM/Rec(2020)1 of the Committee of Ministers to member States on the human rights impacts of algorithmic systems. Appendix. para 2.
[114] Recommendation CM/Rec(2020)1 of the Committee of Ministers to member States on the human rights impacts of algorithmic systems. Appendix. Para 4.
[115] 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.
[116] 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. p4.
[117] 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. p4.

same direction as the Council since the Scottish Biometric Commissioner has a statutory duty to produce a code that will address the acquisition, retention, use and destruction of biometric data for criminal justice and police purposes.[118] That being said, there is much more that can be done to provide a supportive framework for the use of emerging technologies including biometric identification systems.

### 3.5.2.3: Good Practice in Emerging Technology: New Zealand Police

The New Zealand Police have undertaken a great deal of work to reflect on their policing practice in the context of deploying emerging technologies. They developed a New Technology Framework in 2021 that seeks to support decision making in the development of policy, procedures and process involved in the use of new technology in policing.[119] This framework is designed around three mechanisms that ensure a robust framework in implemented. These three mechanisms are a Trial or Adopt New Policing Technology Policy, a New Technology Working Group (of internal members) and an Expert Panel in Emergent Technology (external members).

The policy set out with the following purposes:

1. Ensure decisions to trial or adopt new and evolving policing technologies and technology-enabled capabilities are made ethically and proportionately with individual and community interests

2. Ensure Police's approach aligns with wider New Zealand Government ethical standards and expectations, including the Government Chief Data Steward's and Page Privacy Commissioner's Principles for the safe and effective use of

[118] S7, Scottish Biometrics Commissioner Act 2020, Section 34. The Scottish Biometrics Commissioner's role is marginally limited by s20 of the Protection of Freedoms Act 2012, which affords the Secretary of State the authority to appoint a Commissioner for the Retention and Use of Biometric Material who will address those issues relating to national security.

[119] Policy on Trial or Adoption of New Policing Technology | New Zealand Police

data and analytics and Statistics, and New Zealand's Algorithm Charter for Aotearoa New Zealand

3. Ensure decisions reflect Police's obligations to Te Tiriti o Waitangi including by seeking and taking account of a te ao Māori perspective

4. Enhance public trust and confidence by ensuring decisions and the reasons for them are transparent, and decision-makers are accountable

5. Enable Police to innovate safely, so that opportunities offered by technology to deliver safer communities and better policing outcomes for New Zealanders are not lost.

The development of the policy followed two significant evaluations one by the Law Foundation of New Zealand and the other commissioned by the New Zealand police focusing on the regulation of facial recognition technologies (Lynch et al, 2020: Lynch and Chen, 2021). These reports made a number of recommendations on how to develop an effective legal and ethical framework and while focused on one specific type of technology they raise issues that are likely to permeate developments in emerging technologies.

For example, it was highlighted that the more sensitive the information being processed by a piece of technology the greater protection needed. On a similar vein, the more sensitive the information the greater the need for specific legal structures to authorise that processing and to ensure the necessary reliability, transparency, and accountability. Indeed, the newly developed policy should go some way to addressing the concerns raised by Lynch et al.

As you can see from the framing of the policy purpose a central feature was the recognition of the relationship of the policy to its community and ensuring that all members of the community are represented. In the New Zealand context, this is a

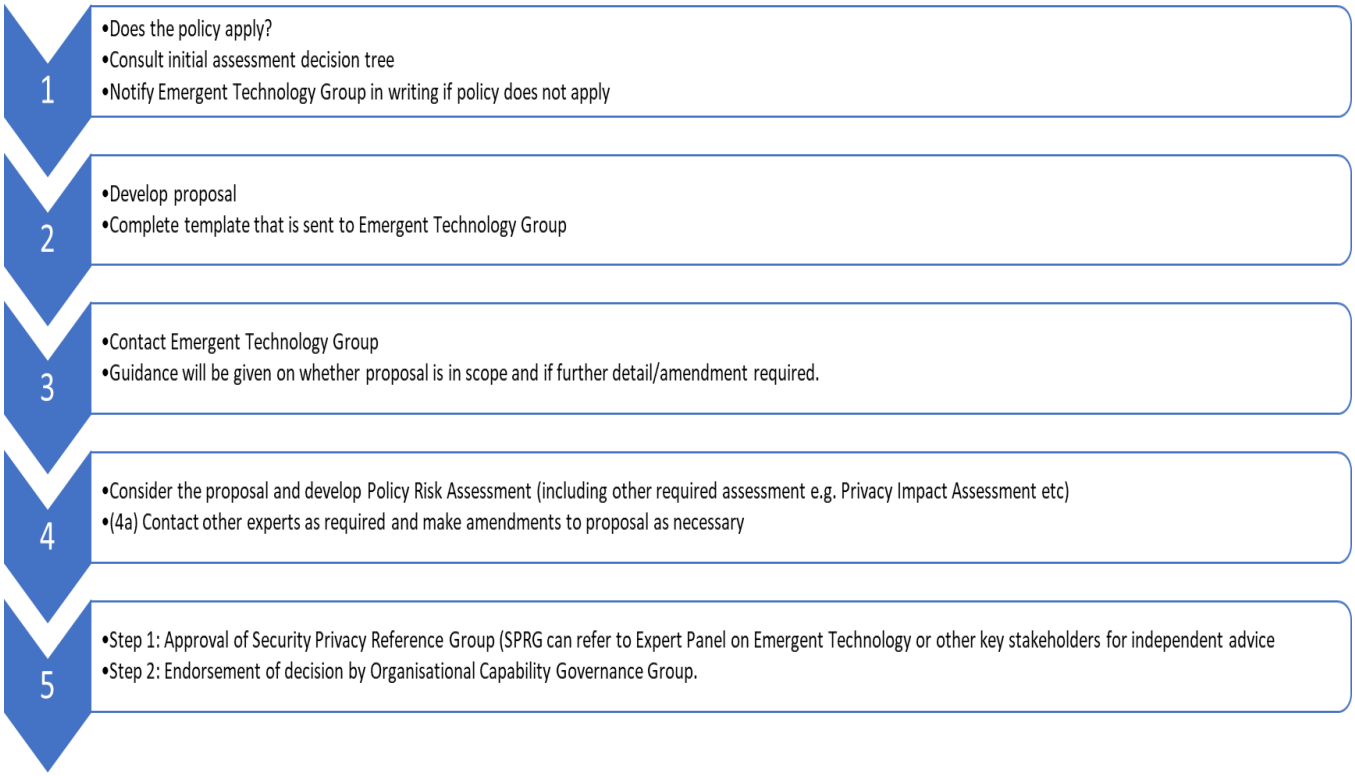
particularly important issue because they have a significant Māori population (Lynch & Chen, 2021, Lynch et al, 2020). Moreover, it has been widely recognised that one of the most persistent features of the use of emerging technology is the potential of their use to exacerbate discriminatory practice (Steege, 2021). By framing the purpose of the policy as set out above there is recognition that there is a need to address this issue on an ongoing basis.

The policy introduces 10 principles that are intended to guide decision making in the trial or adoption of new technology. Those principles are:

| **Principle** | **Description** |
|---|---|
| 1. Necessity | There is a demonstrable need for Police to acquire the capability |
| 2. Effectiveness | There is a good reason to believe the technology will meet the need |
| 3. Lawfulness | The proposed use is lawful |
| 4. Partnership | A te ao Māori perspective, as well as Pacific, and other communities have been considered and affected communities consulted |
| 5. Fairness | Possible data or use biases have been considered and risks mitigated |
| 6. Privacy | Possible data or use biases have been considered and risks mitigated |
| 7. Security | Data and Information security risks have been considered and risks mitigated |
| 8. Proportionality | Individual, group, and wider community impacts have been considered and any negative impacts are proportionate to the necessity and benefits |
| 9. Oversight and accountability | Policy, audit, and reporting controls will assure that the technology is only used as intended. |

| | |
|---|---|
| 10. Transparency | Appropriate information about the technology, its use, and how to challenge adverse outcomes will be publicly available |

The implementation of these principles is secured through a 5-step approval process that must be followed in the trial or adoption of either a new technology-based policing capability, or a new use of an existing technology. This 5-step process is as follows:




The advantage of this process is that it is clearly set out, making it transparent. There are formalised points in the process that allow for the development and refinement of a proposal. Importantly, there are various points at which the expertise of external contributors can be drawn upon and that can provide an independent evaluation of the technology's potential risks and benefits in a policing context. However, a limitation of the process as narrated in the policy is it not clear when an

independent expert is needed and how such an expert should be identified and selected.

The Expert Panel in Emergent Technology's terms of reference establish that its role is to provide external and independent expert scrutiny of, and advice on, Police proposals that involve emergent technology.[120] The Commissioner of the Police appoints the Chair of the panel and in consultation with them appoint the other members. While this may raise questions in terms of the truly independent composition of the panel, there is some degree of transparency secured in that their appointment and expertise is accessible on the New Zealand Police website.[121] The terms of reference do require that a declaration of interest is made but it is at the Chair discretion how that impacts on the individual's participation. Therefore, the visibility of membership on the New Zealand Police website is an important aspect of ensuring accountability. Without such mechanisms there may be the potential for commercial entities to gain influence in the development of technological innovation (or indeed to repress development). Further transparency is embedded in that the terms of reference expressly state that there is presumption that their advice will be made publicly available. However, as yet there is limited evidence of this.

One of the greatest attributes of the New Zealand police's approach is the accessibility of its documentation. The framework and policy documents are easily accessible on its website and as such is available to any citizen who wishes to access it.[122] It is written in a clear language that is easy to follow. However, as the

[120] New Zealand Police Expert Panel on Emergent Technologies, Terms of Reference, May 2021. Available: expert-panel-emergent-technologies-tor.pdf (police.govt.nz).
[121] Advisory panel on emergent technologies | New Zealand Police | New Zealand Police
[122] Police use of emergent technologies | New Zealand Police

policy has only been recently established there is little evidence of how the policy is being implemented and to what extent it is meaningfully incorporated into policing practice.

Within the operation of this framework, there is explicit acknowledgement that where a piece of technology relies substantively on an algorithm consideration should be given to the NZ Police Guidelines for algorithm life-cycle management. This is an important mechanism through which the NZ Police can ensure that they comply with their obligations in terms of the Algorithm Charter.[123] However, it should be noted that this Charter is of a voluntary nature and lacks a mechanism through which compliance can be monitored (Bennett-Moses et al, 2021).

### 3.5.3: Surveillance and Tracking Devices

In Canada they do have a binding framework. The Canadian Directive requires that regulated entities undertake an algorithmic impact assessment prior to adopting systems dependent on them.[124] The tool that they use is open source so you can really see how it works.[125] However, in both the case of the UK guidance and the Canadian provisions the focus is on Government/Public Sector generally as opposed to policing specifically. For this reason, should a compulsory algorithmic impact assessment be considered it would need to be tailored to the policing context.

This is important because algorithms have the potential to mask, exacerbate and escalate human biases and there is currently no minimum scientific or ethical

[123] KM_C554e06673-20200925115807 (police.govt.nz)
[124] Directive in Automated Decision Making, 2019: Directive on Automated Decision-Making- Canada.ca
[125] Algorithmic Impact Assessment Tool - Canada.ca

standards an AI tool must meet before it can be used in the criminal justice system.[126]" It has been suggested by the Justice and Home Affairs Committee that the solution is to establish a national body who can engage in the process of creating such standard.[127] Indeed, since the time of their report there has been some progress on this front with the Alan Turning Institute leading a project seeking to draft global technical standards.[128]

## 4. Concluding Discussion and Recommendations

This review has examined the existing academic, policy-relevant, and legal literature concerning emerging technologies in policing. Specifically, it has examined the existing research and policy-relevant literature to understand the social and ethical implications associated with different types of emerging technologies in policing practice, and the legal considerations that associated with the adoption of these emerging technologies within the context of policing. It has examined the range of recommendations obtained from research and the lessons learnt from elementary application within police practice as specified within the existing research literature concerning policing and has also looked at the recommendations that can be made for informing best practice in policing from trials and the implementation of similar types of emerging technologies in the Health Care and Children and Families institutional settings. Finally, it also explored what recommendations can be made from the analysis of existing case law for the adoption of these technologies within the Scottish policing context.

[126] Justice and Homes Affairs Committee, Technology rules? The advent of new technologies in the justice system, 1st Report of Session 2021–22, HL Paper 180. March 2022. p4.
[127] Justice and Homes Affairs Committee, Technology rules? The advent of new technologies in the justice system, 1st Report of Session 2021–22, HL Paper 180. March 2022. p4.
[128] UK Government, New UK initiative to shape global standards for Artificial Intelligence - GOV.UK (www.gov.uk), Press Release.

As our review was based on two overarching key objectives: 1) the identification of best practice in legislative frameworks and ethical standards, as well as any legislative gaps surrounding emerging technologies and their adoption in policing practice, and 2) the identification of research evidence and best practice for the adoption and implementation of emerging technologies in policing, including for the development and use of ethical guidelines and scientific standards, it thereby contributes to the requirements of Workstreams 1 and 2 and associated Key Focus Areas.

## 4.1: Social and Ethical Issues associated with different forms of Emerging Technologies

The review found that there were a number of distinct as well as overlapping social and ethical issues associated with the three different forms of emerging technologies: electronic databases, biometric identification systems, and surveillance systems and tracking technologies. A full summary of these findings is available in **Table 1 on page 59.**

### 4.1.1: Electronic Databases

The particular social and ethical issues that need to be considered for the adoption and dissemination of electronic database technologies are: the safety of the information held, the issues of human rights and privacy, the need for standardisation and accountability, differences in organisational practices, the potential for bias to be embedded within the data held, public trust, legitimacy, the

management of sensitive data, and the opportunities and risks associated with data collection, sharing and surveillance of vulnerable populations. However, the findings also show that certain particular risks apply to particular types of electronic database technology, but not necessarily to others. Particular issues associated with data sharing and third-party data sharing platforms are those concerning: the safety of information held, human rights and privacy, lack of standardisation and accountability, differences in organisational practice, and the risk of embedded bias in data, data organisation and data sharing processes. Particular issues associated with community policing applications are the risk of enhancing racial inequalities via their use, and the issue of the need to maintain public trust. While issues concerning the lack of alignment in organisational culture, the risks of enhancing both actual and perceived social injustices and legitimacy of police action represent pressing issues for open-source datasets, data pulling platforms, and social media platforms and data storage technologies, the existing research suggests that consideration also needs to be given to the management and use of sensitive information that social media data may hold about particular individuals. The management of vulnerable population data and DNA database technologies are other issues associated with these forms of technologies.

However, the research reveals that far less is known about the particular social and ethical issues associated with open-source data, data pulling platforms and DNA databases than the other types of electronic database technologies, with less empirical research or practice-based reports available for these types of technologies. This suggests this is an area where further research should be

undertaken to ascertain a fuller understanding of the particular ethical and social issues associated with these particular types of emerging technologies.

### 4.1.2: Biometric Identification Systems

As with electronic databases, a range of particular as well as overlapping social and ethical issues were found within the existing research literature focusing on biometric identification technologies and systems. The main social and ethical issues associated with this form of emerging technologies were: trust and legitimacy, accuracy, fairness, and transparency, risks of enhancing social inequalities via deployment of these technologies, privacy and security, the risks of these technologies being deployed by perpetrators of crime, as well as the need for standardisation regarding ethical principles and guidance for their dissemination. Specific issues associated with facial recognition technologies were those of trust and legitimacy, the risk of enhancing social inequalities, privacy and security, and the need for standardised ethical principle and guidance. These issues were also important for artificial intelligence technologies, however, for this particular type of technology, the existing research acknowledged its potential for use in criminal behaviour. Much less is known about the social and ethical issues associated with voice pattern analysis tools, however the limited research available suggests that the main concerns with these forms of technology pertain to human rights and the lack of well-established norms governing the use of AI technology in practice.

### 4.1.3: Surveillance Technologies and Tracking Devices

The key social and ethical issues associated with the implementation, adoption and use of surveillance technologies and tracking devices are: the legitimacy of use by

police departments, public confidence and trust, concern relating to bias, privacy, their effectiveness in reducing crime, the legitimacy of product selection, the lack of guidance or integration of technology within specific crime reduction agendas, as well as their wider implications for public-state relationships and their impacts on police officers and policing practices.

Particular issues associated with the use of drone technologies are: legitimacy, the development of an aerial geopolitics of security, public confidence and trust, concern relating to racial bias, and issues of privacy. Issues of privacy and legitimacy are also well documented in the existing research focusing on smart devices and sensors. The research focusing on the use of body worn cameras discusses the implications of these technologies in relation to public-state relationships, the impacts on police officers and police practices, as well as concerns about racial biases inherent in the deployment of this type of technology. Concern over the lack of clear standards and guidance for the use of technologies was evident throughout the research examining the different types of surveillance technologies. However, the review also revealed that less is known about the social and ethical implications concerning the use of autonomous security robots than other forms of surveillance and tracking technologies, which again suggest that this is a form of emerging technology where further research is needed to explore the social and ethical implications of its use.

### 4.2: Legal Issues Associated with Emerging Technologies

The review found that the main legal issues associated with emerging technologies concern the Law of Evidence, especially in relation to improperly obtained evidence, disclosure of evidence, data protection, and human rights and equality. In particular,

the use of emerging technologies is highly likely to challenge the boundaries of the Criminal Procedure (Sc) Act 1995, Regulation of Investigatory Powers (Scotland) Act 2000, Investigatory Powers Act 2016, as well as compliance with the National Assessment Framework for Biometric Data Outcomes and prospectively the Scottish Biometric Commissioners' Code of Conduct.

The analysis also found that specific legal issues are also associated with the three different forms of emerging technologies. With regards to electronic databases, legal challenges have related to whether the data should be retained, for how long, and at what point should it be deleted. In many respects an overlap exists between the regulation of databases and the operation of biometric identification system as these systems usually require operationalisation through a database. However, the key legal issue with this form of technology is that biometric information is inherently sensitive personal information and therefore requires greater protection. Specific legal concerns associated in relation to automated decision making and the use of artificial intelligence were also identified. Furthermore, regulation of this in the UK is very limited. Another important issue is the lack of a centralised register for artificial intelligence technologies.

### 4.3: Recommendations for Police Practice

Overall, the amount of literature specifying particular evidence-based recommendations from which to develop best practice in the rollout of emerging technologies in policing was more limited than for the body of literature evidencing the social and ethical issues associated with these forms of technology. This in itself represents a particular limitation in the existing body of knowledge and the review

highlights the need for more trials to be undertaken within the policing context from which to develop specific recommendations for informing best practice. The amount of available literature focusing on best practice in relation to the development and implementation of ethical guidelines and scientific standards was limited, especially the amount of material focusing on scientific standards.

4.3.1: Specific Recommendations for Electronic Database Technologies

However, despite the limitations in this area of research, the key recommendations that can be drawn from research focusing on the use of electronic database technologies in police practice are:

- The need for guidelines to ensure that technology does not result in increased victimisation, inequalities and inefficiency in its storage and use,
- The need for greater integration between academic researchers, police, the policy community and third parties to develop and implement specific solutions that are sensitive to the needs of all parties.
- Standardisation of practice with other parts of government who have different cultures and practices regarding the collection, storing, processing and use of data to ensure consistency between the different departments who work in collaboration with the police and to remove the potential for ambiguity regarding access and use of data.
- For assessments to be undertaken to establish best practice and decision making,
- Legal clarity in the form of codes of practice and specific legislation over the legal obligations on data storage and processing across all parties.

- Clarification over consent issues relating to data subjects, particularly who can access the data and for what purpose and data subject consent regarding the use and storage of data held about them
- For the introduction of MASH (Multi-Agency Safeguarding Hubs) to be created to allow for better data sharing practices and partner agencies, underpinned by the development of a clear decision-making framework at the national level to ensure ethical storage, management, and use of data, as well to help safeguard the data on vulnerable individuals
- Specific guidelines for working with social media data, and
- For further research to be undertaken concerning the use of national datasets to gain a better understanding of the risks involved in the use of such technologies.
- Ongoing review and audit to quickly identify and remedy any emerging issues resulting from the use of the technology

It is important to note however, that no specific evidence-based recommendations were provided in the sample literature specifically for data pulling platforms, open-source data, community policing applications, or for DNA databases. This highlights the priority that should be given to conducting research-based trials of the implementation of these types of emerging technologies from which specific recommendations can then be drawn.

Additional recommendations for the implementation of electronic database technologies can be made on the basis of the lessons learnt and recommendations for good practice provided in the literature focusing on the implementations of this

form of emerging technology in the health sector and in the Children and Family sector. The evidence provided here presents important considerations for the implementation of these technologies in policing. From this evidence, it is recommended that:

- Cross sectoral discussion should be undertaken to co-develop guidelines or standards concerning the use of these technologies with minors or to hold data about minors to address concerns around uncertainty
- Guidelines and training should be provided to better prepare professionals on how to write notes and input data
- Specific guidelines are provided to professionals regarding subject access to records held about them.

It is important to acknowledge that the literature reviewed concerning policing practice did not provide any specific recommendations regarding the issue of child rights or child rights assessments specifically in relation to the use of these technologies in the policing context. However, research from the health sector recommends:

- The design and implementation of co-produced guidelines concerning ethical practice for minors to address concerns around uncertainty.

### 4.3.2: Specific Recommendations for Biometric Identification Systems and AI Technologies

Specific recommendations for the adoption of biometric identification systems technologies are:

- The need to proactively improve public support for the use of facial recognition technologies through information to counter biases in media

reporting about the risks, as well as the need to devise new ethical principles and guidelines for the use of these forms of technology.

- The need to interrogate biases and limitations as to the efficiency of these systems were prior to development.
- The provision of guidelines or clear processes for the scrutiny, regulation, and enforcement of biometric identification systems, including facial recognition technologies as part of a new draft code of practice which should specify the responsibilities for policing bodies regarding scrutiny, regulation, and enforcement of these new standards.
- The need for further trials to be conducted to explore the benefits and limitations of the use of facial recognition technologies in different policing activities
- For mandatory equality impact assessments to be introduced, as well as the collection and reporting of ethnicity data, well as the introduction of protections for minority groups
- For the adoption of an Ethics of Care approach to minimise the risk of harm and to improve perceptions of fairness regarding Artificial Intelligence technologies
- 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.
- Development of a national technology clearinghouse for improvement and standardisation in scientific standards
- The use of context-specific evaluation methodologies for statistical algorithms (Oswald 2022)

- Development of a national ethics approach with clear scientific standards written with the policing context in mind

Other important recommendations that can be made for policing from the examination of trials and lessons learnt from the implementation of artificial intelligence technologies in other sectors are:

- For professionals, including third parties, who collaborate with police departments to be involved in the design and implementation of these technologies to help promote ethical awareness and practice through shared expectations and standardisation of requirements concerning their use.
- The use of practice-based, self-reflexive assessments

4.3.3: Specific Recommendations for Surveillance Technologies and Tracking Devices

Key recommendations for best practice in the use of surveillance and tracking technologies derived from the review of the literature focusing on policing practice are:

- For greater training to be provided and for greater emphasis to be given to the behavioural effects that these forms of technology may have on officers,
- For key stakeholders and all members of the public to be involved in the formulation of police guidelines concerning the use of these technologies, especially to democratise the rules around body-worn cameras and reduce controversy regarding their implementation with public and third-party stakeholder.

- For very strict ethical codes and laws to be implemented for the use of autonomous security robotic devices in policing
- For clear standards and principles to be developed concerning the use of these technologies in forensic investigations.

However, the literature did not provide any specific recommendations or examples of good practice in the implementation of drones or new forms smart technologies and devices. Further research should therefore be undertaken to trial the implementation of these forms of emerging surveillance technologies in different policing contexts and activities.

Other recommendations that can be drawn from research and practice in other institutions are for:

- Increased transparency over potential risks of widening socio-economic and racial inequalities
- The implementation of Leslie's (2019) Ethical Considerations for AI Research and Trials – See **Example 5 (box) on Page 107.**

4.3.4: Recommendations for Future Research in the Scottish Policing Context

In addition, while the review examined research concerning the particular social and ethical issues associated with emerging technologies and trialling of these forms of technologies in policing practice and in other sectors across a range of geographic and governance contexts, namely Scotland, England and Wales, the United States, Canada, Australia and New Zealand, the amount of evidence-based research focusing specifically on the Scottish context remains limited. This highlights the need for further research to be undertaken examining the specific ethical and social issues

associated with these all the different forms of technologies and how they manifest within the Scottish context, as well as to conduct trials of these technologies within the Scottish policing context. Another key recommendation would therefore be:

- For further research to be conducted focusing on emerging technologies and their application within Scottish society and the Scottish policing context.

4.3.5: Recommendations from the Review of the Legal Literature and Case Law

Additional recommendations can also be drawn from the review of the legal literature and case law. Specific recommendations for legislation, policy and practice are:

- Legislation: Designing a measure which makes an algorithmic impact assessment prior to the use of that algorithm compulsory. (Example can be taken from the Canadian Directive on Automated Decision Making).
- Policy: Development of an algorithmic impact assessment policy. One should be tailored to algorithms used in an administrative context and the other should focus on the context of algorithmic connected to operational decision making.
- Policy: Develop a policy on the trial and adoption of new technology policy. Example can be taken from the New Zealand Police.
- Practice: For templates to be developed to implement the algorithmic impact assessment. Examples can be seen in the UK Transparency template and the Canadian Algorithmic Impact Assessment.

In the completion of an algorithmic impact assessment and a data protection impact assessment the following should be addressed: a) The relationship between those involved in the development and implementation of emerging technologies should be

mapped. This is critical to being able to determine roles and responsibilities in the protection of personal information. This is of particular significance when data is being shared between organisations and that data is transferred from the private sector to the public sector or vice versa. b) The understanding of the nature of the data that is being processed and the scope of that processing. This will have a knock-on effect on the lawful basis of processing, the need for consent and in turn, the information that needs to be provided to the data subject. In addition, it will impact on the degree of risk to an individual who is the subject of an algorithmic decision.

- Practice: Staff should be trained in how to engage critically with the adoption and use of new technologies (particularly AI enabled technologies) so that they are in a position to meaningfully engage in the impact assessments noted above.

In addition, it also would be beneficial to explore in more detail the experience of the New Zealand police's role out of their new technology policy, as well as to examine how the use of AI technologies in the collection and use of evidence and intelligence interacts with law of evidence examining how the integration of AI technologies in policing impact on public trust and confidence in the police. These therefore present potential avenues for future research.

### 4.4: Summary of the Recommendations for Research, Policy, Legislation and Practice for Different Types of Emerging Technologies (Table)

The recommendations for best practice for each type of emerging technology as well as for those applicable across all types of emerging technology can be summarised

and grouped according to whether these recommendations are aimed at research, legislation and policy, or practice. Categorising the recommendations in this way can help decision-making concerning the actioning of these recommendations by the different stakeholders. **Table 4** presents a summary of the recommendations for all and specific types of emerging technology and indicates which of recommendations are aimed at research, policy and legislation, and practice.

| Table 4: Summary of Recommendations for Each Type of Emerging Technology | | |
|---|---|---|
| **Type of Emerging Technology** | **Focus** | **Recommendations** |
| **All Types of Emerging Technology** | Research | 1. 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.<br>2. The relationship between those involved in the development and implementation of emerging technologies should be mapped for data protection purposes. There is also a need to understand the nature of the data being processed and the scope of that processing<br>3. Future research should examine 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 |
| | Policy | 1. An equality and human rights impact assessment should form a compulsory part of the trial and adoption of any new technology policy. |
| | Practice | 1. A monitoring mechanism should be incorporated into the design and implementation of an emerging technology to record data on its equality and human rights impacts<br>2. Training should be given 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<br>3. Data on the equality impacts of trial use of technologies should be made publicly available |
| **Electronic Databases** | Research | 1. Further research should be undertaken concerning the use of national datasets<br>2. 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.<br>3. Trials and assessments to establish best practice and decision making within a range of policing contexts in Scotland and the UK |

| | | |
|---|---|---|
| | Policy & Legislation | 1. MASH (Multi-Agency Safeguarding Hubs) should be developed and implemented to allow for better data sharing practices with partner agencies, which should be underpinned by the development of a clear decision-making framework at the national level to ensure ethical storage, management, and use of data, as well to help safeguard the data on vulnerable individuals.<br>2. Standardised guidelines should be developed and implemented to ensure that technology does not result in increased victimisation, inequalities and inefficiency in its storage and use.<br>3. For careful mapping of data flows to be undertaken to ensure that roles within the data protection framework can be established and legal obligations complied with.<br>4. Where consent is not the ground on which lawful processing is based, the processing must be necessary for the performance of a task carried out for law enforcement purposes, or if for sensitive data, there must be an appropriate policy document in place<br>5. The Data Protection Act 2018 gives a very narrow definition of law enforcement purposes and so, where a database is being used for purposes beyond that scope, consideration needs to be given to the lawful basis of processing<br>6. Development of specific guidelines for working with social media data<br>7. Cross sectoral discussion to co-develop guidelines or standards concerning the use of these technologies with minors or to hold data about minors. |
| | Practice | 1. Standardardisation of practice with professionals from other government sectors (e.g. health, social work) regarding the collection, storing, processing and use of data.<br>2. Guidance and training to prepare professionals working in policing and other sectors that work closely with members of the police on how to write notes and input data to ensure greater standardization of practice<br>3. Specific guidelines should be provided for police and closely affiliated professionals regarding subject access to records and data held about them. |
| **Biometric Identification Systems & AI** | Research | 1. Research to explore the benefits and limitations of the use of facial recognition technologies in different policing activities.<br>2. 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 discussion of social and ethical issues of the use of AI.<br>3. 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<br>4. The interrogation of biases and limitations as to the efficiency of AI systems prior to development. |

| | | |
|---|---|---|
| | | 5. For police professionals and other parties that work closely with the police to be involved in the design and implementation of these technologies to help promote ethical awareness and practice. |
| | Policy & Legislation | 1. To improve general public support for the use of facial recognition technologies as well as the need to devise new ethical principles and guidelines for their use of these forms of technology.<br>2. Development and provision of guidelines or clear processes for the scrutiny, regulation, and enforcement of biometric identification systems, including facial recognition technologies as part of a new draft code of practice which should specify the responsibilities for policing bodies regarding scrutiny, regulation, and enforcement of these new standards.<br>3. Introduction of mandatory equality impact assessments<br>4. Development of a national ethical approach that includes clear scientific standards for these forms of technology.<br>5. Establish a national technology clearinghouse for ensuring robust scientific standards for AI technologies.<br>6. Development of policy for trial and adoption of new technologies.<br>7. Introduction of a measure which makes an algorithmic impact assessment prior to the use of that algorithm compulsory |
| | Practice | 1. Adoption of an Ethics of Care approach.<br>2. Development of templates to implement algorithmic impact assessments.<br>3. Staff training to enable meaningful engagement in impact assessments |
| **Surveillance Technologies & Tracking Systems** | Research | 1. Trials to explore the benefits and limitations of the use of these different forms of technology in different policing contexts. |
| | Policy & Legislation | 1. For key stakeholders and members of the public to be involved in the formulation of police guidelines concerning the use of these technologies.<br>2. For very strict ethical codes and laws to be implemented for the use of autonomous security robotic devices in policing<br>3. For clear standards and principles to be developed concerning the use of these technologies in forensic investigations. |

| | | |
|---|---|---|
| | Practice | 1. Training to be provided and consideration given to the behavioural effects that these forms of technology can have on officers |

### 4.5: Next Steps for Further Research

To further address the existing research limitations concerning the specific social and ethical implications associated with emerging technologies in policing in the Scottish context, a supplementary, qualitative research study should be undertaken with personnel involved in policing. This could involve conducting interviews with professionals involved in policing activities or sending out a series of questions to project partners to explore their views and experiences of emerging technologies and to find out about the benefits of the use of these technologies and the issues encountered with the implementation and/or use of specific technologies in the Scottish policing context. Another avenue that could be explored is the opportunities and challenges encountered in relation to the use of these technologies during the Covid-19 pandemic.

**References**

Aicardi, C., Fothergill, T., Rainey, S., Carsten Stahl, B., and Harris, E., (2018), Accompanying technology development in the Human Brain Project: From foresight to ethics management, Futures 102, 114-124. https://doi.org/10.1016/j.futures.2018.01.005

Aizenberg, E., & van den Hoven, J. (2020). Designing for human rights in AI. Big Data & Society. https://doi.org/10.1177/2053951720949566

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

Asante K., Owen R., and Williamson G. (2014) Governance of New Product Development and Perceptions of Responsible Innovation in the Financial Sector: Insights from an Ethnographic Case Study, Journal of Responsible Innovation, 1: 9–30.

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. (2021) 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., 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.

Backman, C., & Löfstrand, C. H. (2021). Representations of Policing Problems and Body-Worn Cameras in Existing Research. International Criminal Justice Review. https://doi.org/10.1177/10575677211020813

Bargenda, J.A., & Wilson-Stark, S. (2018). The legal Holy Grail? German lessons on codification for a fragmented Britain. Edin L R 22(2) 183-210

Barrett, D., & Heale, R. (2020). What are Delphi Studies? Evidence-based nursing 23(3), 68–69. https://doi.org/10.1136/ebnurs-2020-103303

Beck, R. A., (2021). Artificial Intelligence, Predictive Policing, and Risk Assessment for Law Enforcement, Annual Review of Criminology 4. 1, 209-237.

Bennett Moses, Lyria and Valentine, Kylie and Chan, Janet, Data Practices in a Web of Values: Reflections on the Gap between Ethical Principles and Data-Driven Social Policy (October 1, 2021). Janet Chan and Peter Saunders (eds), Big Data for Australian Social Policy (Academy of Social Sciences in Australia, 2021) 105-119, UNSW Law Research Paper No. 21-76, Available at SSRN: https://ssrn.com/abstract=4054085

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

Black, A. & Lumsden, K. (2020) Precautionary policing and dispositives of risk in a police force control room in domestic abuse incidents: an ethnography of call handlers, dispatchers and response officers, Policing and Society, 30, 1, 65-80, DOI: 10.1080/10439463.2019.1568428

Blease C, Kaptchuk T. J., Bernstein, M. H, Mandl, K. D., Halamka, J. D., Des Roches, C. M., (2019). Artificial Intelligence and the Future of Primary Care: Exploratory Qualitative Study of UK General Practitioners' Views, J Med Internet Res, 21, (3):e12802, doi: 10.2196/12802

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

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

Bradford, B., Aston, E., O'Neill, M. and Wells, H. (2022), 'Virtual Policing' trust and legitimacy. I n J. Terpstra, R. Salet, & N. R. Fyfe (Eds.), *The Abstract Police: Critical reflections on contemporary change in police organisations*. Eleven International Publishing. Pp. 213-238.

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

Brandt, T., Dlugosch, O., Abdelwahed, A., van den Berg, P. L., Neumann D. (2021). Prescriptive Analytics in Urban Policing Operations, Manufacturing and Service Operations Management, DOI: 10.1287/msom.2021.1022

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

Brey, P. (2012). Anticipating Ethical Issues in Emerging IT. Ethics and Information Technology, 14, 4. 305–317

Brey, P. (2017). Ethics of Emerging Technologies. In S. O. Hansson (Ed.), Methods for the Ethics of Technology. Rowman and Littlefield International.

Bromberg, D. E., Charbonneau, E., & Smith, A. (2020). Public support for facial recognition via police body-worn cameras: Findings from a list experiment, Government Information Quarterly, 37, 1, https://doi.org/10.1016/j.giq.2019.101415.

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

Bryman, A. (2012). Social Research Methods (4th edition), Oxford University Press, United States.

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

Catte, R., & Linden, R., (2021). Leadership and Change in Winnipeg's Smart Policing Initiative, Policing: A Journal of Policy and Practice, 15, 1, 181-196. DOI: 10.1093/police/pay077

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

Cuomo, D., & Dolci, N. (2021). New tools, old abuse: Technology-Enabled Coercive Control (TECC), Geoforum, 126, 224-232, https://doi.org/10.1016/j.geoforum.2021.08.002

Custers, B. (2012). Technology in policing: Experiences, obstacles and police needs, Computer Law & Security Review, 28, 1 62-68, https://doi.org/10.1016/j.clsr.2011.11.009

Custers, B. & Vergouw, B., (2015), Promising policing technologies: Experiences, obstacles and police needs regarding law enforcement technologies, Computer Law & Security Review, 31, 4, 518-526, https://doi.org/10.1016/j.clsr.2015.05.005

Dalkey, N., & Helmer, O. (1963). An experimental application of the Delphi method to the use of experts. Management Science 9, 458- 467. doi:10.1287/mnsc.9.3.458.

Davis, J.M., & Garb, Y. (2020). Toward Active Community Environmental Policing: Potentials and Limits of a Catalytic Model, Environmental Management 65, 3, 385-398 DOI: 10.1007/s00267-020-01252-1

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

Dunlop, J., Chechak, D., Hamby, W., & Holosko, M. J., (2021) Social Work and Technology: Using Geographic Information Systems to Leverage Community

Development Responses to Hate Crimes, Journal of Technology in Human Services, DOI: 10.1080/15228835.2021.1931635

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

Ekaabi, M. A., Khalid, K., Davidson, R., Kamarudin, A. H., Preece, C. (2020), Smart policing service quality: conceptualisation, development and validation, Policing: An International Journal of Police Strategies and Management, 43, 5, 707-721. DOI: 10.1108/PIJPSM-03-2020-0038

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

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

Fussey, P., and Murray, D. (2019), Independent Report on the London Metropolitan Police Service's Trial of Live Facial Recognition Technology, University of Essex Human Rights, http://repository.essex.ac.uk/24946/.

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

Gaelle, K. & Joëlle, V., (2018), How Could the Ethical Management of Health Data in the Medical Field Inform Police Use of DNA? Frontiers in Public Health, DOI=10.3389/fpubh.2018.00154

Gramagila, J.A., & Phillips, S.W. (2018). Police Officers' Perceptions of Body-Worn Cameras in Buffalo and Rochester. American Journal of Criminal Justice 43, 313–328 https://doi.org/10.1007/s12103-017-9403-9

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

Grimond, W., and Singh, A., (2020), A Force for Good: Results from FOI requests on artificial intelligence in the police force. Royal Society for the encouragement of Arts, Manufactures and Commerce. https://www.thersa.org/globalassets/reports/2020/a-force-for-good-police-ai.pdf

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

Healey, K. and Stephens, N. (2017), Augmenting justice: Google glass, body cameras, and the politics of wearable technology, Journal of Information, Communication and Ethics in Society, 15, 4, 370-384. https://doi.org/10.1108/JICES-04-2016-0010

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

Henman, P. (2019) Of algorithms, Apps and advice: digital social policy and service delivery, Journal of Asian Public Policy, 12, 1, 71-89, DOI: 10.1080/17516234.2018.1495885

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

Huff, J., Katz, C.M. & Webb, V.J. (2018), Understanding police officer resistance to body-worn cameras, Policing: An International Journal, 41, 4, 482-495. https://doi.org/10.1108/PIJPSM-03-2018-0038

Jacob K., Nielsen L., and van den Hoven M. J. (2013) Options for Strengthening Responsibile Research and Innovation. Report of the Expert Group on the State of Art in Europe on Responsible Research and Innovation (Expert Group Report No. EUR25766 EN). Reseach and Innovation, p. 78. Luxembourg: European Commission

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

Kendall, K.E. (1997), The Significance of Information Systems Research on Emerging Technologies: Seven Information Technologies that Promise to Improve Managerial Effectiveness. Decision Sciences, 28: 775-792. https://doi.org/10.1111/j.1540-5915.1997.tb01331.x

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

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

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.

Kuo, P. F., & Lord, D., (2019), A promising example of smart policing: A cross-national study of the effectiveness of a data-driven approach to crime and traffic safety, Case studies on Transport Policy, 7, 4, 761-771. DOI: 10.1016/j.cstp.2019.08.005

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

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

Liebert, W., and Schmidt J. C., (2010) Collingridge's Dilemma and Technoscience: An Attempt to Provide a Clarification from the Perspective of the Philosophy of Science, Poiesis & Praxis, 7: 55–71.

L'Hoiry, X., Moretti, A. & Antonopoulos, G.A. (2021), Identifying sex trafficking in Adult Services Websites: an exploratory study with a British police force. Trends Organ Crim. https://doi.org/10.1007/s12117-021-09414-1

Lum, C., Koper, C. S., & Willis, J. (2017). Understanding the Limits of Technology's Impact on Police Effectiveness. Police Quarterly, 20, 2, 135–163. https://doi.org/10.1177/1098611116667279

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

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

Marchant, G. (2011) The Growing Gap Between Emerging Technologies and the Law. Chapter 2 in Marchant, G., Allenby, B.R. and Herkert, J.R., (eds) The Growing Gap Between Emerging Technologies and Legal-Ethical Oversight (Dorfrecht, Germany: Springer) pp19-32.

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

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

Moon, H., Choi, H., Lee, J., & Lee, K. S. (2017), Attitudes in Korea toward Introducing Smart Policing Technologies: Differences between the General Public and Police Officers. Sustainability, 9, 10, 1921. https://doi.org/10.3390/su9101921

Moses, L.B. (2013) How to Think about Law, Regulation and Technology: Problems with ‘Technology’ as a Regulatory Target, Law, Innovation and Technology, 5:1, 1-20, DOI: 10.5235/17579961.5.1.1

Mugari, I., & Obioha, E. E. (2021), Predictive Policing and Crime Control in The United States of America and Europe: Trends in a Decade of Research and the Future of Predictive Policing. Social Sciences, 10, 6, 234. https://doi.org/10.3390/socsci10060234

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

Oh, G., Zhang, Y., & Greenleaf, R. G. (2021). Measuring Geographic Sentiment toward Police Using Social Media Data. American Journal of Criminal Justice, https://doi.org/10.1007/s12103-021-09614-z

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

Paterson, C., & Clamp, K. (2014), Innovating Responses to Managing Risk: Exploring the Potential of a Victim-Focused Policing Strategy, Policing: A Journal of Policy and Practice, 8, 1, 51-58. DOI: 10.1093/police/pat028

Powell, A., & Henry, N. (2018) Policing technology-facilitated sexual violence against adult victims: police and service sector perspectives, Policing and Society, 28, 3, 291-307, DOI: 10.1080/10439463.2016.1154964

Ray, R., Marsh, K., & Powelson, C. (2017), Can Cameras Stop the Killings? Racial Differences in Perceptions of the Effectiveness of Body-Worn Cameras in Police Encounters. Sociological Forum, 32: 1032-1050. https://doi.org/10.1111/socf.12359

Rigano, C., (2019), Using Artificial Intelligence to Address Criminal Justice Needs, NIJ Journal 280, https://www.nij.gov/journals/280/Pages/using-artificialintelligence-to-address-criminal-justice-needs.asp

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

Rosenfeld, A., (2019). Are drivers ready for traffic enforcement drones? Accident Analysis & Prevention, 122, 199-206, https://doi.org/10.1016/j.aap.2018.10.006.

Sahin, N. M., & Cubukcu, S. (2021), In-Car Cameras and Police Accountability in Use of Force Incidents. J Police Crim Psych. https://doi.org/10.1007/s11896-021-09472-9

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

Sandhu, A., & Fussey, P. (2021) The 'uberization of policing'? How police negotiate and operationalise predictive policing technology, Policing and Society, 31, 1, 66-81, DOI: 10.1080/10439463.2020.1803315

Sandhu, A., & Haggerty, K. D. (2017). Policing on camera. Theoretical Criminology, 21, 1, 78–95. https://doi.org/10.1177/1362480615622531

Saulnier, A, Lahay, R, McCarty, W. P., & Sanders, C. (2020), The RIDE study: Effects of body-worn cameras on public perceptions of police interactions. Criminol Public Policy, 19: 833– 854. https://doi.org/10.1111/1745-9133.12511

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

Singh, M. (2017) Mobile technologies for police tasks: An Australian study, Journal of Organizational Computing and Electronic Commerce, 27, 1, 66-80, DOI: 10.1080/10919392.2016.1263114

Skogan, W. G., & Hartnett, S. M. (2005) The Diffusion of Information Technology in Policing, Police Practice and Research, 6, 5, 401-417, DOI: 10.1080/15614260500432949

Sleigh, J., and Vayena, E. (2021), Public engagement with health data governance: the role of visuality. Humanit Soc Sci Commun 8, 149 https://doi.org/10.1057/s41599-021-00826-6

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

Smykla, J. O., Crow, M. S., Crichlow, V. J. et al. (2016), Police Body-Worn Cameras: Perceptions of Law Enforcement Leadership. Am J Crim Just, 41, 424–443 https://doi.org/10.1007/s12103-015-9316-4

Snilstveit, B., Oliver, S. & Vojtkova, M. (2012). Narrative approaches to systematic review and synthesis of evidence for international development policy and practice, Journal of Development Effectiveness 4(3), 409-29. https://doi.org/10.1080/19439342.2012.710641

Sollie, P. (2007). Ethics, Technology Development and Uncertainty: An Outline for any Future Ethics of Technology. Journal of Information, Communications & Ethics in Society, 5,4, 293–306.

Stahl, B. C., (2012) Morality, Ethics and Reflection: A Categorisation of Normative Research in IS Research, Journal of the Association for Information Systems, 13: 636–56.

Stahl, B. C., Timmermans, J., Flick, C., (2017), Ethics of Emerging Information and Communication Technologies: On the implementation of responsible research and innovation, Science and Public Policy, 44, 3: 369–381, https://doi.org/10.1093/scipol/scw069

Steege, H. (2021), Algorithm-based Discrimination by Using Artificial Intelligence: Comparative Legal Considerations and Relevant Areas of Application. 1: 56-71.

Stone, K. E. (2018), Smart Policing and the Use of Body Camera Technology: Unpacking South Africa's Tenuous Commitment to Transparency, Policing: A Journal of Policy and Practice, 12, 1, 109-115, DOI: 10.1093/police/pax066

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

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

Todd, C., Bryce, J., & Franqueira, V. N. L. (2021) Technology, cyberstalking and domestic homicide: informing prevention and response strategies, Policing and Society, 31, 1, 82-99, DOI: 10.1080/10439463.2020.1758698

Tulumello, S., & Iapaolo, F., (2021), Policing the future, disrupting urban policy today. Predictive policing, smart city, and urban policy in Memphis, Urban Geography, DOI: 10.1080/02723638.2021.1887634

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

Urquhart, L., Miranda, D., & Podoletz, L. (2022). Policing the smart home: The internet of things as 'invisible witnesses'. *Information Polity*. https://doi.org/10.3233/IP-211541

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

van 't Wout, E., Pieringer, C., Irribarra, D. T., Asahi, K., & Larroulet, P. (2021) Machine learning for policing: a case study on arrests in Chile, Policing and Society, 31, 9, 1036-1050, DOI: 10.1080/10439463.2020.1779270

Veale, M., (2019), Algorithms in the Criminal Justice System, The Law Society of England and Wales, https://michae.lv/static/papers/2019algorithmsjusticesystem.pdf

Vilendrer, S., Armano, A., Johnson, C. G. B., Favet, M., Safaeimli, N., Villasenor, J., Shaw, J. G., Hertelendy, A. J., Asch, S. M., & Mahoney, M. (2021), An App-Based Intervention to Support First Responders and Essential Workers During the COVID-

19 Pandemic: Needs Assessment and Mixed Methods Implementation, Journal of Medical Internet Research, 23, 5, e26573 DOI: 10.2196/26573.

Wall, T. (2016) Ordinary Emergency: Drones, Police, and Geographies of Legal Terror. Antipode, 48, 1122– 1139. doi: 10.1111/anti.12228

Ross, M., Chalmers, J. & Callander, I. (2020). Walker and Walker: The Law of Evidence. (5th Edition, Bloomsbury Professional).

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

Weaver, C. M., Chu, J. P., Lugo, A., Uyeda, N., Cha, Y. M., Zadonowics, T., & Giordano, B. (2021). Community-Based Participatory Research With Police: Development of a Tech-Enhanced Structured Suicide Risk Assessment and Communication Smartphone Application, Law and Human Behavior, 45, 5, 456-467. DOI: 10.1037/lhb0000470

White, M. D., Todak, N., & Gaub, J. E. (2018), Examining Body-Worn Camera Integration and Acceptance Among Police Officers, Citizens, and External Stakeholders. Criminology & Public Policy, 17, 649-677. https://doi.org/10.1111/1745-9133.12376

Whitehead, S., & Farrell, G., (2008), Anticipating Mobile Phone 'Smart Wallet' Crime: Policing and Corporate Social Responsibility, Policing: A Journal of Policy and Practice, 2, 2, 210–217, https://doi.org/10.1093/police/pan024

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

Wienroth, M., (2020), Value beyond scientific validity: let's RULE (Reliability, Utility, LEgitimacy), Journal of Responsible Innovation, DOI: 10.1080/23299460.2020.1835152.

Williams, A., & Paterson, C. (2021). Social Development and Police Reform: Some Reflections on the Concept and Purpose of Policing and the Implications for Reform in the UK and USA, Policing: A Journal of Policy and Practice, 15, 2, 1565–1573, https://doi.org/10.1093/police/paaa087

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

Wilson-Kovacs, D. (2021), Digital media investigators: challenges and opportunities in the use of digital forensics in police investigations in England and Wales, Policing: An International Journal, 44, 4, 669-682. https://doi.org/10.1108/PIJPSM-02-2021-0019

Wright, J. (2021). Suspect AI: Vibraimage, Emotion Recognition Technology and Algorithmic Opacity. Science, Technology and Society. https://doi.org/10.1177/09717218211003411

Wright, D., and Friedewald, M., (2013), Integrating privacy and ethical impact assessments, Science and Public Policy, 40, 6: 755–766, https://doi.org/10.1093/scipol/sct083

Urquhart, L., Miranda, D. Podoletz, L. (2022) Policing the smart home: The internet of things as 'invisible witnesses', Information Polity, 27, 2: 233-246.

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

# Appendices

## Appendix 1: Emerging Technologies and Analytical Framework for Emerging Technologies

### Defining Emerging Technologies: Some Thoughts

The term 'emerging technologies' has gained traction in recent years in different public service and policy environments. Use of the term is quite fluid, in that it is used in relation to a range of technologies, usually digital technologies, and in a number of different contextual settings. In the context of policing, many of these emerging technologies facilitate new information flows in and around the institutions of policing, and in doing so impact on internal structures and citizen-police interactions. Examples of emerging technologies in policing would include: Automatic Face Recognition (AFR), Body-Worn Video (BWV) Cameras, Artificial Intelligence (AI), Profiling and Drones.

### Text-Book definition

The term emerging technologies is generally used to describe a new technology, but it may also refer to the evolution of an existing technology, and it can have different meanings when used in different areas, such as media, business, science, or public services. The term commonly refers to technologies that are currently developing, or that are expected to be implemented in the next five to ten years, and is usually reserved for technologies that are creating, or are expected to create, significant social, institutional or economic impacts.

Emerging digital technologies are usually perceived to offer new business and service opportunities, whilst at the same time posing challenges to existing ways of doing things, these include legal and ethical challenges, and for digital technologies these often relate to data processes and data protection. For public services, such as those agencies involved in policing policy and practice, such data processes are likely to involve the personal data of citizens and will have a bearing on citizen-state relations.

When thinking about what constitutes an emerging technology there are some important definitional issues to consider:

### The Nature of the Technology

Emerging technologies in contemporary discourse are usually assumed to be digital technologies supporting new information flows embedded in new information and communication technologies (ICTs). In this respect, such technologies involve data, including personal data, and data flows. Whilst emerging technologies may be defined by their digital component, they do not have to be exclusively digital and can comprise of other elements, including physical features. Philosophically, any physical artefact can be considered a technology, from the humble pencil through to satellite weaponry.

### Technological Components of Emerging Technologies

Emerging technologies are usually a configuration of a range of technological artifacts and are not really a single technology. For example, a surveillance camera system

would include a camera, a network, monitors, and recording and storage equipment. As such, and emerging technology is really an assemblage of different components. So, when we talk about an emergent technology, we are not necessarily talking about the individual components of the technology, but often their combined integration into a new 'technology' or application. BWV is a good example of this. The emergent technology may derive from the convergence of a number of technological developments including: computerisation, miniaturisation and/or enhanced technological capability/capacity.

**The Emergent Aspect of Emerging Technologies**

Given that emerging technologies comprise of a number of different components it is unsurprising to suggest that not all of the components are new or emerging and many have been in existence for a number of years. The emergent element of these technologies is their combination into a new application or artefact, or their introduction into a new service area. Looking beyond the technical artefact, emerging technologies can also be considered emergent, in that they facilitate emerging new informational relationships and ways of working. So, it may not be the technology that is new, but its introduction into a new service area, and the impacts that the technology has in that service area. Alternatively, it may be the case that an emergent technology has existed for many years, but that a new application has become envisioned that had not previously been foreseen.

**The Point of Emergence**

Emerging technologies are often at a different point of emergence. Some may be envisioned, but not yet in existence, others in development, or being trialled, whilst others are at the point of implementation, yet are still considered to be emerging. There is a body of academic work around innovation theory and cycles, and technological maturity. It may be that an emerging technology has been around for years, but that it has only recently diffused into a specific service setting.

**Implications and Consequences**

By definition, the full impact and consequences associated with the use of emergent technologies is not known and the implication of their use is uncertain and ambiguous. There may be perceived benefits of their use that do not materialise, or unintended consequences that do. Moreover, sometimes the visions bestowed on technologies by their advocates, in terms of what they will deliver, does not emerge in practice.

**Analytical Framework for Emerging Technologies**

A simple analytical framework can be devised to take account of the above points and to draw out the key features of an emerging technology.

**Analytical Framework for Emerging Technologies**

| | Technological Components | Technological Purpose | Technological Maturity | Institutional Context | Data Flows | Challenges |
|---|---|---|---|---|---|---|
| | What technological components does the emerging tech consist of? | What is the specified purpose of the tech? What are the perceived benefits? | How long has the tech been in existence? Is it used elsewhere? | What service or policy arena is it to be used in? Who uses the tech? | What data is created and how it is used? What are the emergent service relations embodied in the tech? | What are the perceived challenges associated with using the tech (including legal and ethical challenges)? |
| **Emerging Technology A** | | | | | | |
| **Emerging Technology B** | | | | | | |
| **Emerging Technology B** | | | | | | |

## Appendix 2: Lists of References and Abstracts of Document Selected for Inclusion

Part A: List of Abstracts Selected for Inclusion in Final Pool of Academic Research Articles

1. Abbas, N. & Policek, N. (2021) ‘Don’t be the same, be better’: an exploratory study on police mobile technology resistance, *Police Practice and Research*, 22, 1, 849-868, DOI: 10.1080/15614263.2020.1728271.

Abstract

Purpose: This contribution stems from the acknowledgment that the post-adoptive officers' behaviour and utilisation of the mobile technology has not yet been examined. Between 2008 - 2010, the Home Office funded the Mobile Information Programme to increase the visibility of police officers and increase the efficiency and effectiveness of the Police Service. This programme had enabled the roll-out of 41,000 mobile devices to police officers, allowing them to spend a greater percentage of their working time out of police stations. Yet, in 2012, the NPIA's evaluation of the increase in police officers' visibility showed that on average, officers spent around 18 minutes extra per shift out of the station using mobile devices. Methodology: To overcome the paucity of available data, a pilot study adopting a multi-method approach was conducted in a medium-sized constabulary in the UK. Data collection methods included focus groups, Q cards methodology and an online survey. Findings: This study sheds light on officers' main reasons for post-adoptive resistance to using the mobile devices and its impact on the quality of police data recorded. Furthermore, it delineates innovative ways of enhancing police mobile technology training to boost technology adoption in police forces.

2. Aizenberg, E., & van den Hoven, J. (2020). Designing for human rights in AI. *Big Data & Society*. https://doi.org/10.1177/2053951720949566

Abstract

In the age of Big Data, companies and governments are increasingly using algorithms to inform hiring decisions, employee management, policing, credit scoring, insurance pricing, and many more aspects of our lives. Artificial intelligence (AI) systems can help us make evidence-driven, efficient decisions, but can also confront us with unjustified, discriminatory decisions wrongly assumed to be accurate because they are made automatically and quantitatively. It is becoming evident that these technological developments are consequential to people's fundamental human rights. Despite increasing attention to these urgent challenges in recent years, technical solutions to these complex socio-ethical problems are often developed without empirical study of societal context and the critical input of societal stakeholders who are impacted by the technology. On the other hand, calls for more ethically and socially aware AI often fail to provide answers for how to proceed beyond stressing the importance of transparency, explainability, and fairness. Bridging these socio-technical gaps and the deep divide between abstract value language and design requirements is essential to facilitate nuanced, context-dependent design choices that will support moral and social values. In this paper, we bridge this divide through the framework of Design for Values, drawing on methodologies of Value Sensitive Design and Participatory Design to present a roadmap for proactively engaging societal stakeholders to translate fundamental human rights into context-dependent design requirements through a structured, inclusive, and transparent process.

3. 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

Abstract

Machine Learning has become a popular tool in a variety of applications in criminal justice, including sentencing and policing. Media has brought attention to the possibility of predictive policing systems causing disparate impacts and exacerbating social injustices. However, there is little academic research on the importance of fairness in machine learning applications in policing. Although prior research has shown that machine learning models can handle some tasks efficiently, they are susceptible to replicating systemic bias of previous human decision-makers. While there is much research on fair machine learning in general, there is a need to investigate fair machine learning techniques as they pertain to the predictive policing. Therefore, we evaluate the existing publications in the field of fairness in machine learning and predictive policing to arrive at a set of standards for fair predictive policing. We also review the evaluations of ML applications in the area of criminal justice and potential techniques to improve these technologies going forward. We urge that the growing literature on fairness in ML be brought into conversation with the legal and social science concerns being raised about predictive policing. Lastly, in any area, including predictive policing, the pros and cons of the technology need to be evaluated holistically to determine whether and how the technology should be used in policing.

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

Abstract

The rapid development of facial recognition technologies (FRT) has led to complex ethical choices in terms of balancing individual privacy rights versus delivering societal safety. Within this space, increasingly commonplace use of these technologies by law enforcement agencies has presented a particular lens for probing this complex landscape, its application, and the acceptable extent of citizen surveillance. This analysis focuses on the regulatory contexts and recent case law in the United States (USA), United Kingdom (UK), and European Union (EU) in terms of the use and misuse of FRT by law enforcement agencies. In the case of the USA, it is one of the main global regions in which the technology is being rapidly evolved, and yet, it has a patchwork of legislation with less emphasis on data protection and privacy. Within the context of the EU and the UK, there has been a critical focus on the development of accountability requirements particularly when considered in the context of the EU's General Data Protection Regulation (GDPR) and the legal focus on Privacy by Design (PbD). However, globally, there is no standardised human rights framework and regulatory requirements that can be easily applied to FRT rollout. This article contains a discursive discussion considering the complexity of the ethical and regulatory dimensions at play in these spaces including considering data protection and human rights frameworks. It concludes that data protection impact assessments (DPIA) and human rights impact assessments together with greater transparency, regulation, audit and explanation of FRT use, and application in

individual contexts would improve FRT deployments. In addition, it sets out ten critical questions which it suggests need to be answered for the successful development and deployment of FRT and AI more broadly. It is suggested that these should be answered by lawmakers, policy makers, AI developers, and adopters.

5. Anania, E. C., Rice, S., Pierce, M., Winter, S. R., Capps, J., Walters, N. W., and Milner, M. N. (2019). Public support for police drone missions depends on political affiliation and neighborhood demographics, *Technology in Society*, 57, 95-103, https://doi.org/10.1016/j.techsoc.2018.12.007.

Abstract

Background: As unmanned aerial systems (UAS) become more common, it is important to understand public opinion and support for these UAS. The current research attempts to investigate support for law enforcement usage of UAS, and the factors affecting this support.

Methods: A three-study mixed methods approach was taken. In the first study, participants responded to questions asking their level of support for police UAS usage in neighborhoods with varying racial compositions, as well as answering free response questions related to the scenario. The second and third study investigated support for police UAS usage, and whether or not this was influenced by participants' political affiliation.

Results: Study one indicated that participants displayed significantly more support for law enforcement's use of UAS when flying over a predominately African-American neighborhood than when flying over a primarily Caucasian neighborhood. Study two furthered these results by finding that those identifying as liberal showed less

support for law enforcement UAS use and expressed higher levels of privacy concerns than those identifying as conservative. Study three further investigated political affiliation using the Nolan Chart survey, finding that libertarians, liberals, conservatives, and authoritarians had differing levels of support and privacy concerns.

Conclusions: This research adds to a foundation of understanding consumer acceptance and support for law enforcement UAS usage. As this practice becomes more common, it is important to understand support, as individual perceptions will likely influence actions. This work has numerous practical applications for policy and design.

6. 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

Abstract

Police use-of-force continues to be a major source of international concern, inviting interest from academics and practitioners alike. Whether justified or unnecessary/excessive, the exercise of power by the police can potentially tarnish their relationship with the community. Police misconduct can translate into complaints against the police, which carry large economic and social costs. The question we try to answer is: do body-worn-cameras reduce the prevalence of use-of-force and/or citizens' complaints against the police? We empirically tested the use of body-worn-cameras by measuring the effect of videotaping police-public

encounters on incidents of police use-of-force and complaints, in randomized-controlled settings. Over 12 months, we randomly assigned officers to "experimental-shifts" during which they were equipped with body-worn HD cameras that recorded all contacts with the public and to "control-shifts" without the cameras (n = 988). We nominally defined use-of-force, both unnecessary/excessive and reasonable, as a non-desirable response in police-public encounters. We estimate the causal effect of the use of body-worn-videos on the two outcome variables using both between-group differences using a Poisson regression model as well as before-after estimates using interrupted time-series analyses. We found that the likelihood of force being used in control conditions were roughly twice those in experimental conditions. Similarly, a pre/post analysis of use-of-force and complaints data also support this result: the number of complaints filed against officers dropped from 0.7 complaints per 1,000 contacts to 0.07 per 1,000 contacts. We discuss the findings in terms of theory, research methods, policy and future avenues of research on body-worn-videos.

7. 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

Abstract:

The adoption of data-driven organizational management - which includes big data, machine learning, and artificial intelligence (AI) techniques - is growing rapidly across all sectors of the knowledge economy. There is little doubt that the collection, dissemination, analysis, and use of data in government policy formation, strategic planning, decision execution, and the daily performance of duties can improve the

functioning of government and the performance of public services. This is as true for law enforcement as any other government service.

8. Asaro. P. (2016). "Hands up, don't shoot!": HRI and the automation of police use of force. *Journal of. Human-Robot Interactions*. 5, 3, 55–69. https://doi.org/10.5898/JHRI.5.3.Asaro

Abstract

This paper considers the ethical challenges facing the development of robotic systems that deploy violent and lethal force against humans. While the use of violent and lethal force is not usually acceptable for humans or robots, police officers are authorized 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. With the increased interest in developing and deploying robots for law enforcement tasks, including robots armed with weapons, the question arises as to how to design human-robot interactions (HRIs) in which violent and lethal force might be among the actions taken by the robot, or whether to preclude such actions altogether. This is what I call the "deadly design problem" for HRI. While it might be possible to design a system to recognize various gestures, such as "Hands up, don't shoot!," there are many more challenging and subtle aspects to the problem of implementing existing legal guidelines for the use of force in law enforcement robots. After examining the key legal and technical challenges of designing interactions involving violence, this paper concludes with some reflections on the ethics of HRI design raised by automating the use of force in policing. In light of the serious challenges in automating violence, it calls upon HRI researchers to adopt a moratorium on designing any robotic systems that deploy violent and lethal force

against humans, and to consider ethical codes and laws to prohibit such systems in the future.

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

Abstract

The literature on the importance of procedural justice in policing is extensive. Using the context of information sharing in community policing, this paper argues that interactional, procedural and distributive justice are salient in interactions between the police and the public, both online and face-to-face. Structured interviews (n = 161) were conducted with members of young minority groups and intermediaries (who work with minorities and police agencies) across nine countries in Europe. Our analysis of barriers and facilitators to sharing information with the police highlights processes of interactional, procedural and distributive justice in building public confidence. We highlight theoretical and practical implications of relevance to policing internationally. Our findings show that demonstrating aspects of interactional justice (attitude and behaviour, accessibility and communication, personal contact and relationships); procedural justice (responsiveness and efficiency, data protection and security); and distributive justice (outcomes and effectiveness, equity in distribution of policing services) have a role in building public confidence and facilitating information sharing with police online and face-to-face. We conclude that in addition to micro-level interactions, meso-level social processes (e.g. community

policing models and data protection and security procedures) can be useful in enhancing public confidence.

10. Backman, C., & Löfstrand, C. H. (2021). Representations of Policing Problems and Body-Worn Cameras in Existing Research. *International Criminal Justice Review*. https://doi.org/10.1177/10575677211020813

Abstract

In this article, we analyze scholarly publications on body-worn cameras (BWCs) to shed light on scholars' grounding assumptions about BWC technology and the policing problems assumed to be amended by it. We conducted a systematic search and a double-blind review, including 90 peer-reviewed journal articles, and analyzed how scholars warrant their studies, their findings and their recommendations. We found that BWC research largely investigates the effectiveness of BWCs worn by police officers in the United States and build upon a set of dominant policing problem representations: the police crisis in the United States and the police use of force, lack of oversight and control of police officers, citizen dissatisfaction and lack of police legitimacy, and police officer resistance toward BWC use. Assumptions underlying all four problem representations is that BWC technology will amend these problems and is legitimate and useful if the public supports it. Taken together, this enhances the representation of BWC technology as a self-evident means of improving community relations and police legitimacy in the United States. Finally, we provide recommendations for future research on BWCs, particularly the need for research departing from altogether different problem representations.

11. Beck, R. A., (2021). Artificial Intelligence, Predictive Policing, and Risk Assessment for Law Enforcement, *Annual Review of Criminology* 4. 1, 209-237.

Abstract

There are widespread concerns about the use of artificial intelligence in law enforcement. Predictive policing and risk assessment are salient examples. Worries include the accuracy of forecasts that guide both activities, the prospect of bias, and an apparent lack of operational transparency. Nearly breathless media coverage of artificial intelligence helps shape the narrative. In this review, we address these issues by first unpacking depictions of artificial intelligence. Its use in predictive policing to forecast crimes in time and space is largely an exercise in spatial statistics that in principle can make policing more effective and more surgical. Its use in criminal justice risk assessment to forecast who will commit crimes is largely an exercise in adaptive, nonparametric regression. It can in principle allow law enforcement agencies to better provide for public safety with the least restrictive means necessary, which can mean far less use of incarceration. None of this is mysterious. Nevertheless, concerns about accuracy, fairness, and transparency are real, and there are tradeoffs between them for which there can be no technical fix. You can't have it all. Solutions will be found through political and legislative processes achieving an acceptable balance between competing priorities.

12. Black, A. & Lumsden, K. (2020) Precautionary policing and dispositives of risk in a police force control room in domestic abuse incidents: an ethnography of call handlers, dispatchers and response officers, *Policing and Society*, 30, 1, 65-80, DOI: 10.1080/10439463.2019.1568428

Abstract

This article explores the riskwork engaged in by call handlers, dispatchers and response officers in a police force control room in England. We present a novel approach by drawing on the work of Foucault and his concept le dispositif to study riskwork in policing in a post-austerity landscape and to develop the analytical concept of 'precautionary policing'. Dispositional analysis allows us to focus on social dispositions or inclinations and to demonstrate how these arrangements affect social interaction and organisational behaviour. We draw on data collected via ethnographic fieldwork focusing on domestic abuse incidents in a police force control room in England. The findings focus on: (1) organisational technologies of risk, which guided and surfaced staff actions and decision-making; (2) riskwork to mitigate and manage threats and harm to victims and the public; and (3) riskwork relating to the professional decision-making of individual staff and officers. In addition to bringing the risk tools and artefacts 'into being' through their (inter-)actions, for staff, these technologies are a safety net to justify practices. They erode opportunities for officer discretion, particularly in relation to responses to domestic incidents. Therefore, despite policy discussions of the need to reduce officers' risk aversion and reduce unnecessary bureaucracy, a risk averse culture still pervades. Uncertainty becomes a justification for pre-emptive action by officers and staff before risks become known, and demonstrates a shift to precautionary policing practices which do not follow the blueprints of risk management.

13. 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

Abstract

I bring an understanding of the concept and practice of “aversive racism” to scholarly thinking about community formation. I argue that the exclusionary contours of community are in part a product of racialized in- and outgrouping from which people’s capacities for place-making are judged and localized policing is instigated. In bringing these concepts, formations, and practices together, this paper contributes to how urbanists might continue to think about the role of race in displacement, particularly as it plays out in the context of neighborhood change and gentrification more broadly. In the penultimate section I provide a discussion of the popular Nextdoor app as a means of illustrating a contemporary example of community-instigated policing and platform for what Dána-Ain Davis calls “muted racism.”

14. 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

Abstract

Facial recognition technology is just one of a suite of new digital tools police and other security providers around the world are adopting in an effort to function more safely and efficiently. This paper reports results from a major new London-based study exploring public responses to Live Facial Recognition (LFR): a technology that enables police to carry out real-time automated identity checks in public spaces. We

find that public trust and legitimacy are important factors predicting the acceptance or rejection of LFR. Crucially, trust and, particularly, legitimacy seem to serve to alleviate privacy concerns about police use of this technology. In an era where police use of new technologies is only likely to increase, especially as the Covid-19 global pandemic develops, these findings have important implications for police–public relations and how the 'public voice' is fed into debates.

15. Braga, A. A., & Schnell, C., (2013). Evaluating Place-Based Policing Strategies Lessons Learned from the Smart Policing Initiative in Boston, *Police Quarterly*, 16, 3, 339-357. DOI: 10.1177/1098611113497046.

Abstract: In response to an increase in violent crime during the mid-2000s, the Boston Police Department implemented the Safe Street Teams program to control "hot spots" that generated a disproportionate amount of violence in Boston through the use of community and problem-oriented policing interventions. Like many police programs, the Safe Street Teams strategy was not implemented with a commitment to conduct a program evaluation. The Smart Policing Initiative provided the Boston Police with an important opportunity to partner with academic researchers to perform retrospective process and impact evaluations. Quantitative and qualitative methods were used to analyze the concentration and stability of violent crime in targeted places, examine the integrity of program implementation, and conduct a rigorous quasi-experimental analysis of program impacts. These research products established the crime control effectiveness of the Safe Street Teams and assisted the Boston Police in strengthening the implementation of the program.

16. 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

Abstract

Facial recognition technology (FRT) offers police a fast, efficient, and accurate way of identifying criminals. However, as with any new technology, the public is often sceptical about how the police will use this technology and how it may impinge on the public's privacy and security. Subsequently, if police use of FRT is perceived as illegitimate, police-citizen relationships may deteriorate - this is especially concerning given the current lack of trust and confidence in police as expressed in the Black Lives Matter movement and other protests against police actions. This paper takes a novel approach to examining public opinions and attitudes about the use of FRT by police. To do this, we thematically analysed 609 public commentary posts published on 71 YouTube clips about police use of FRT. We found that the public in this sample expressed mostly negative sentiments about the use of FRT by police, identifying three main concerns: authority and power, technology, rights and freedoms. However, we also found some support for police using FRT. These findings are discussed in terms of the theoretical concept of the new regulatory state; in particular steering (government policy) and rowing (implementation). These findings suggest that if police authorities and policy makers address these specific concerns by being transparent in their practices and educate the public about misinformation, then policing agencies may have an increase support for the use of FRT by police and, moreover, build trust and confidence in police.

17. Brandt, T., Dlugosch, O., Abdelwahed, A., van den Berg, P. L., Neumann D. (2021). Prescriptive Analytics in Urban Policing Operations, *Manufacturing and Service Operations Management*, DOI: 10.1287/msom.2021.1022.

Abstract:

Problem definition: We consider the case of prescriptive policing, that is, the data-driven assignment of police cars to different areas of a city. We analyze key problems with respect to prediction, optimization, and evaluation as well as trade-offs between different quality measures and crime types. Academic/practical relevance: Data-driven prescriptive analytics is gaining substantial attention in operations management research, and effective policing is at the core of the operations of almost every city in the world. Given the vast amounts of data increasingly collected within smart city initiatives and the growing safety challenges faced by urban centers worldwide, our work provides novel insights on the development and evaluation of prescriptive analytics applications in an urban context. Methodology: We conduct a computational study using crime and auxiliary data on the city of San Francisco. We analyze both strong and weak prediction methods along with two optimization formulations representing the deterrence and response time impact of police vehicle allocations. We analyze trade-offs between these effects and between different crime types. Results: We find that even weaker prediction methods can produce Pareto-efficient outcomes with respect to deterrence and response time. We identify three different archetypes of combinations of prediction methods and optimization objectives that constitute the Pareto frontier among the configurations we analyze. Furthermore, optimizing for multiple crime types biases allocations in a way that generally decreases single type performance along one outcome metric but can improve it along the other. Managerial implications: Although optimization integrating

all relevant crime types is theoretically possible, it is practically challenging because each crime type requires a collectively consistent weight. We present a framework combining prediction and optimization for a subset of key crime types with exploring the impact on the remaining types to support implementation of operations-focused smart city solutions in practice.

18. Bratton, W. J., & Malinowski, S. W., (2008), Police Performance Management in Practice: Taking COMPSTAT to the Next Level, Policing: *A Journal of Policy and Practice,* 2, 3, 259–265, https://doi.org/10.1093/police/pan036

Abstract

William J. Bratton is Chief of the Los Angeles Police Department and former Chief of the NYPD. He is best known for leading the development and expansion of COMPSTAT, the internationally acclaimed command accountability system that uses computer-mapping technology and timely crime analysis to target emerging crime patterns and coordinate police response. Sean W. Malinowski, Ph.D., is a Lieutenant with the LAPD serving as the Assistant Commanding Officer of the LAPD's Real-time Analysis and Critical Response Division. He is a senior fellow with Long Island University's Homeland Security Management Institute. In this article, they consider police performance management in practice, through the lens of Chief Bratton's own experience of reducing crime in New York and Los Angeles. By measuring the performance of police managers whilst holding them to account for crimes, they explain the role COMPSTAT played in fighting crime in these areas and look forward to see how police can continue to innovate and expand upon existing police performance measures.

19. Brayne, S., & Christin, A. (2021), Technologies of Crime Prediction: The Reception of Algorithms in Policing and Criminal Courts, *Social Problems*, 68, 3, 608–624, https://doi.org/10.1093/socpro/spaa004

Abstract

The number of predictive technologies used in the U.S. criminal justice system is on the rise. Yet there is little research to date on the reception of algorithms in criminal justice institutions. We draw on ethnographic fieldwork conducted within a large urban police department and a midsized criminal court to assess the impact of predictive technologies at different stages of the criminal justice process. We first show that similar arguments are mobilized to justify the adoption of predictive algorithms in law enforcement and criminal courts. In both cases, algorithms are described as more objective and efficient than humans' discretionary judgment. We then study how predictive algorithms are used, documenting similar processes of professional resistance among law enforcement and legal professionals. In both cases, resentment toward predictive algorithms is fueled by fears of deskilling and heightened managerial surveillance. Two practical strategies of resistance emerge: foot-dragging and data obfuscation. We conclude by discussing how predictive technologies do not replace, but rather displace discretion to less visible—and therefore less accountable—areas within organizations, a shift which has important implications for inequality and the administration of justice in the age of big data.

20. 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

Despite broad and often varied underlying definitions, a common theme throughout community and neighbourhood policing strategies establishes the need to target improvements in the relationship and level of engagement between the police and the communities they serve. Community policing approaches have long underpinned a desire to move away from reactive policing models towards those which establish a more proactive philosophy, responsive to the wants and needs of the community. The near ubiquitous proliferation of smartphones and other ICTs (Information and Communication Technologies) means they are often seen as a vector through which initiatives of all kinds can instil a culture of proactive engagement with their respective stakeholder communities. This paper builds upon existing research which suggests that technologies for crime prevention should be designed to support communications and problem-solving rather than used simply as a means to disseminate information, unpacking a number of the core concepts that are considered central to participation and effective engagement; social capital, public participation and social and digital inclusion. Moreover, examples of wider initiatives are comparatively discussed, not just those associated with community policing, which target the engagement of communities through the use of technology, and more specifically mobile applications, before reflecting on the empirical evidence and experiences gleaned through the EU H2020 funded ‘UNITY’ project, a project that sought to establish effective strategies for engagement between police and citizen communities.

21. Bromberg, D. E., Charbonneau, E., & Smith, A. (2020). Public support for facial recognition via police body-worn cameras: Findings from a list experiment, Government Information Quarterly, 37, 1, https://doi.org/10.1016/j.giq.2019.101415.

Abstract

Emerging technologies like facial recognition have the potential to change the delivery of public services, but also to reshape the notion of citizenship. The factors influencing the consent of the governed matters to gauge if this specific surveillance technology might be deployed further. The Technology Acceptance Model (TAM) has identified social norms as a contributor to technology adoption. We test social norms for the adoption of facial recognition technology based on an experiment with a sample of residents of New Hampshire through a phone survey, and with a sample of Americans via a web survey. The experiment estimates the overt and real support for facial recognition through police body-worn cameras. Our results are that gender, age and political affiliation matters to explain support for facial recognition via BWC, as females and non-Trump voters harbor reticence that they only express when provided with a measure of anonymity.

22. 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

Abstract

Drawing upon quantitative and qualitative data gathered during a four-year ethnographic study of 44 British homicide investigations, this paper advances the

sparse literature on how closed-circuit television (CCTV) contributes to criminal investigations and the risks associated with its use. Based on insights gleaned from interviews with homicide detectives, analysis of case files and observations of live homicide investigations, we examine how CCTV is used during homicide investigations focusing principally on two key investigative moments - identifying and charging suspects. Our quantitative data indicate that CCTV is used more frequently than any other kind of forensic science or technology to both identify and charge suspects. Nevertheless, our qualitative data reveal numerous challenges associated with how CCTV footage is recovered, viewed, shared, interpreted and packaged for court. We reveal the individual and organisational processes and workarounds that have emerged in a socio-technical landscape that lacks clear standards and principles. We discuss the implications of these findings for practice and policy and their relevance to questions about the socially constructed nature of forensic scientific knowledge.

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

Abstract

There has been optimism that social media will facilitate citizen participation and transform the communication strategies of public organisations. Drawing on a case study of the public police in England, this article considers whether social media are transforming or normalising communications. Arguing that social media have not yet served to facilitate interaction between constabularies and citizens in the ways that have been proposed and desired, the article considers factors that structure the

transformative potential of social media. It is argued that the uses of social media are mediated by the existing organisational and occupational concerns of the police. This article reveals how an interplay of organisational, technological and individual and cultural dynamics come together to shape how social media are used in constabularies. Embedding social media into police communications is challenging and the technology itself will not bring about the organisational and cultural changes needed to transform police–citizen engagement.

24. Carter, J. G., & Grommon, E. (2017) Officer perceptions of the impact of mobile broadband technology on police operations. *Policing and Society* 27, 8, 847-864.

Abstract

Research examining police departments' use of technology is underdeveloped relative to other areas of policing. This gap in the literature is troubling as policing models are becoming more data-driven and thus, relying more heavily on information technologies. Arguably, the most commonly utilised technology in policing practice, and examined in policing research, has been mobile computers. However, there has been little insight into the technological advancement in data communications that directly influence the functionality of mobile computers. This research seeks to inform this shortcoming by examining a police department that implemented a dedicated wireless mobile broadband system. A mixed-methods approach is employed within a medium-sized department in the northeast region of the USA. Survey data were gathered from 76 uniformed police personnel. Semi-structured interviews were conducted with key personnel to further contextualise survey results. Survey results suggest tentative support for improved time savings and execution of

job tasks after the implementation of wireless broadband. Perceptions of mobile broadband impacts on information flow, quality, and accessibility appear positive. Considerations for future research and study limitations are discussed.

25. Catte, R., & Linden, R., (2021). Leadership and Change in Winnipeg's Smart Policing Initiative, Policing: A Journal of Policy and Practice, 15, 1, 181-196. DOI: 10.1093/police/pay077.

Abstract:

If evidence-based policing is to be successful, we need to know more about how leaders can successfully introduce change into their organizations. This study looks at a Smart Policing Initiative (SPI) implemented by the Winnipeg Police Service. Line officers and management personnel were interviewed to determine how they dealt with the implementation of SPI. We used activity data to determine whether officers actually carried out the activities integral to the SPI programme. The research concludes that there was attitudinal 'buy-in' to the programme and that the officers did carry out the proactive policing activities mandated by the programme.

26. 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

Abstract

Technology is pervasive in current police practices, and has been for a long time. From CCTV to crime mapping, databases, biometrics, predictive analytics, open source intelligence, applications and a myriad of other technological solutions take centre stage in urban safety management. But before efficient use of these

applications can be made, it is necessary to confront a series of challenges relating to the organizational structures that will be used to manage them, to their technical capacities and expectations, and to weigh up the positive and negative external factors at play at the intersection between technology, society and urban management. The paper contributes to this discussion by looking into the dynamics that drive technological uptake in the field of urban safety, the different theories underpinning the relationship between crime and space, and the history and technological characteristics of Geographic Information Systems to later present specific case studies and practical examples of crime mapping systems. Finally, addressing matters related to organisational constraints, technological possibilities and societal impact from a critical point of view, the paper lays out guidelines to ensure that using technology to manage urban safety does not result in increased victimisation, inequalities or inefficiency. Taking one of the longest established technology used in police practice, crime mapping, and using a multidisciplinary, critical approach to escape technological solutionism and bridge the gap between the academic literature (STS, urban sociology, environmental criminology) and policy needs and recommendations, this paper sends a cautionary tale to those hoping that technology alone can solve complex urban and social problems.

27. Cuomo, D., & Dolci, N. (2021). New tools, old abuse: Technology-Enabled Coercive Control (TECC), Geoforum, 126, 224-232, https://doi.org/10.1016/j.geoforum.2021.08.002.

Abstract

This paper examines how domestic violence abusers utilize digital technologies to extend their spatial and temporal control over survivors. By highlighting how digital

technologies have become central tools for abusers to threaten, stalk, harass and surveil their partners, we situate technology-enabled coercive control as a continuation of harm perpetrated by domestic violence abusers, rather than a new or distinct form of abuse. Drawing on qualitative interviews conducted in Seattle with survivors, advocates, law enforcement officers and prosecutors, we show how digital technologies enable abusers to more efficiently and effectively coercively control survivors anywhere and at any time, including after the relationship has ended. This paper contributes to geographic scholarship analyzing the role of digital technologies in policing and surveillance and advances this literature through a feminist geographic analytic that offers an embodied accounting of the way digital technologies regulate, discipline and govern at the scale of the body and within intimate relationships.

28. Custers, B. (2012). Technology in policing: Experiences, obstacles and police needs, *Computer Law & Security Review*, 28, 1 62-68, https://doi.org/10.1016/j.clsr.2011.11.009.

Abstract

Increasing efforts are made by police forces all over the world to optimize the use of technology in policing and remove any obstacles as new and existing technologies provide new opportunities for law enforcement, criminal investigation and prosecution. This contribution describes results of research on which technologies are currently used at police forces and other criminal investigation organizations in the Netherlands, their experiences with these technologies and their needs and preferences in this regard. For existing opportunities the prevalence and satisfaction of several technologies in policing, including wiretapping, fingerprints, DNA research,

database coupling, data mining and profiling, camera surveillance and network analyses were investigated. For new opportunities the most promising technologies (i.e., promising according to the police forces) were mapped. Furthermore, an inventory was made of the legal, technological and organizational obstacles police forces encounter when using different technologies for purposes like law enforcement, criminal investigation and prosecution.

29. Custers, B. & Vergouw, B., (2015), Promising policing technologies: Experiences, obstacles and police needs regarding law enforcement technologies, *Computer Law & Security Review*, 31, 4, 518-526, https://doi.org/10.1016/j.clsr.2015.05.005

Abstract

Police forces and law enforcement agencies in many countries are continuously trying to optimize the use of technologies in policing and law enforcement. Efforts are being made to remove existing technological, legal and organizational obstacles to create more opportunities of promising technologies, both existing and new. This contribution describes the results of a survey among 46 police forces and other law enforcement agencies in 11 countries. Their experiences with policing technologies and their needs and preferences in this regard are described. The prevalence and satisfaction of existing technologies, including wiretapping, fingerprints, DNA research, database coupling, data mining and profiling, camera surveillance and network analyses were investigated. Legal, technological and organizational obstacles for the use of technology in policing were mapped and the extent to which policing technologies are evaluated and yield success stories was investigated. The main obstacles, according to the respondents, are insufficient financial resources

and insufficient availability of technology. One in four organizations is lacking any clear, appealing success stories and half of the respondents indicated they were not performing any evaluations on the effectiveness of using particular technologies in policing. As a result, the information available on whether technologies in policing are actually working is very limited.

30. Daly, A., Mann, M., Squires, P., & Walters, R. (2021) 3D printing, policing and crime, *Policing and Society*, 31, 1, 37-51, DOI: 10.1080/10439463.2020.1730835

Abstract

This article examines the implications of advanced manufacturing technology, more commonly known as three dimensional (3D) printing, for policing and crime, notably the dissemination of digital design files and the use of 3D printers to produce illicit firearms. The application and rapid evolution of 3D printing technology has created new challenges for law and regulation, and represents an interesting security paradox, albeit one which until now has received scant attention in the criminological or policing literature. On the one hand, 3D printing denotes a significant shift in the creation and use of objects, ranging from food to body parts, and more controversially, weaponry. On the other hand, the use of this technology to create items such as firearms and weapons signifies a potential safety, security, and legal challenge. We explore the emergence of 3D printing and its use to create firearms along with the theoretical challenges to legal design and enforcement presented by this decentralised technology. We also present some empirical data on instances of 3D printed firearms and firearm parts being detected internationally, and some jurisdictions' legal and policy responses. We conclude by considering that any

regulation of 3D printed firearms must be based on a robust evidence base and take proper account of citizens' rights, but also that any national regulation will be in tension with the transnational and decentralised nature of the technology.

31. Davis, J.M., & Garb, Y. (2020). Toward Active Community Environmental Policing: Potentials and Limits of a Catalytic Model, *Environmental Management* 65, 3, 385-398 DOI: 10.1007/s00267-020-01252-1

Abstract:

This paper offers a field-tested community environmental policing model to address the pressing environmental management challenges of reducing e-waste burning in informal e-waste hubs, and enforcement against informal polluting industries more broadly. This is based on our intervention to reduce e-waste burning in a substantial informal e-waste hub in the West Bank, Palestine, a 45 km(2) region in which an estimated 5-10 metric tonnes of cables are burnt daily, causing serious environmental and public health consequences. In analogous e-waste hubs in the global South, environmental management solutions have focused on economically attractive alternatives to replace cable burning or policies that integrate informal recyclers with formal e-waste management systems-achieving little success. Our paper describes a two-pronged intervention in Palestine's e-waste hub, which reduced e-waste burning by 80% through a combination of economically competitive cable grinding services and an "active" community environmental policing initiative that lowered barriers to and successfully advocated for governmental policing of e-waste burning. Our discussion of this intervention addresses the community environmental policing literature, which has documented few successes stories of real improvements to the enforcement of environmental violations. We argue that

existing strategies have relied on "passive" approaches comprised of monitoring and reporting environmental violations to advocate for change. Our strategy offers a template to improve outcomes through a more "active" approach, moving from monitoring environmental violations through understanding the rationale and dynamics of violators, identifying environmental policing barriers, and implementing a feasible and persuasive strategy to overcome them.

32. Deckert, A., Long, N. J., Aikman, P. J., Appleton, N. S., Graham Davies, S., Trnka, S., Fehoko, E., Holroyd, E., Jivraj, N., Laws, M., Martin-Anatias, N., Pukepuke, R., Roguski, M., Simpson, N., Sterling, R., & Tunufa'l, L. (2021) 'Safer communities … together'? Plural policing and COVID-19 public health interventions in Aotearoa New Zealand, *Policing and Society*, 31, 5, 621-637, DOI: 10.1080/10439463.2021.1924169

Abstract

International media have praised Aotearoa New Zealand for its response to the coronavirus pandemic. While New Zealand Police played a fundamental role in enforcing pandemic control measures, the policing landscape remained plural. This article employs Loader [2000. Plural policing and democratic governance. Social and legal studies, 9 (3), 323-345] model of plural policing to understand responses to public health emergencies. It identifies two forms of policing which were evident in Aotearoa during the COVID-19 lockdown that should be added to Loader's model. First, we argue that contexts with colonial history require that the model not only includes by-government and below-government policing but also next-to-government policing by Indigenous peoples - such as the 'community checkpoints' run by Maori. Second, and further developing Loader's model, we argue that the category of

below-government policing be expanded to include 'peer-to-peer policing' in which government responsibilizes members of the public to subject each other to large-scale surveillance and social control. Since plural forms of policing affect each other's functionality and legitimacy, we argue that what happens at the synapses between policing nodes has profound implications for the process of community building. Because community building is essential to fighting pandemics, we conclude that the policing of pandemic intervention measures may require an expanded understanding and practice of plural policing to support an optimal public health strategy.

33. Degeling, M., & Berendt, B. (2018), What is wrong about Robocops as consultants? A technology-centric critique of predictive policing. *AI & Soc* 33, 347–356 https://doi.org/10.1007/s00146-017-0730-7

Abstract

Fighting crime has historically been a field that drives technological innovation, and it can serve as an example of different governance styles in societies. Predictive policing is one of the recent innovations that covers technical trends such as machine learning, preventive crime fighting strategies, and actual policing in cities. However, it seems that a combination of exaggerated hopes produced by technology evangelists, media hype, and ignorance of the actual problems of the technology may have (over-)boosted sales of software that supports policing by predicting offenders and crime areas. In this paper we analyse currently used predictive policing software packages with respect to common problems of data mining, and describe challenges that arise in the context of their socio-technical application.

34. Duarte, D. E., (2021), The Making of Crime Predictions: Sociotechnical Assemblages and the Controversies of Governing Future Crime, Surveillance and Society, 19, 2, 199-215.

Abstract:

We are witnessing an upsurge in crime forecasting software, which supposedly draws predictive knowledge from data on past crime. Although prevention and anticipation are already embedded in the apparatuses of government, going beyond a mere abstract aspiration, the latest innovations hold out the promise of replacing police officers' "gut feelings" and discretionary risk assessments with algorithmic-powered, quantified analyses of risk scores. While police departments and private companies praise such innovations for their cost-effective rationale, critics raise concerns regarding their potential for discriminating against poor, black, and migrant communities. In this article, I address such controversies by telling the story of the making of CrimeRadar, an app developed by a Rio de Janeiro-based think tank in partnership with private associates and local police authorities. Drawing mostly on Latour's contributions to the emerging literature on security assemblages, I argue that we gain explanatory and critical leverage by looking into the mundane practices of making and unmaking sociotechnical arrangements. That is, I address the chain of translations through which crime data are collected, organized, and transformed into risk scores. In every step, new ways of seeing and presenting crime are produced, with a significant impact on how we experience and act upon (in)security.

35. Dunlop, J., Chechak, D., Hamby, W., & Holosko, M. J., (2021) Social Work and Technology: Using Geographic Information Systems to Leverage Community Development Responses to Hate Crimes, *Journal of Technology in Human Services*, DOI: 10.1080/15228835.2021.1931635

Abstract

This study highlights technology use in community development showing how social workers, police, and neighborhood residents promote safer neighborhoods. The approach used was geographic information systems (GIS) to target specific neighborhoods characterized as needing timely interventions. GIS is a technological sub-specialty and form of spatial cartography allowing data to be stored, manipulated, and visually displayed. This article focuses on how social workers can apply such approaches to enhance their communities and neighborhood residents. We offer a case study of a hate crimes project in Canada that brought together university researchers and a local police service into a research project, designed to identify specific neighborhood places where hate crimes were occurring. We propose that community social workers can form meaningful partnerships with technology experts and leverage this relationship into an expanded practice skill with tangible improvements to the communities they work with.

36. 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

Abstract

For several years now, crime prediction software operating on the basis of data analysis and algorithmic pattern detection has been employed by police departments

throughout the world. As these technologies aim at forestalling criminal events, they may aptly be understood as elements of preventive strategies. Do they also initiate a logic of preemptive policing, as several authors have suggested? Using the example of crime prediction software that is used in German-speaking countries, the article shows how current forms of predictive policing echo classical modes of risk calculation: usually employed in connection with domestic burglary, they help police to identify potential high-risk areas by extrapolating past crime patterns into the future. However, preemptive elements also emerge, to the extent that the software fosters 'possibilistic' thinking in police operations. Moreover, current advances in crime prediction technologies give us a quite different picture of a probable future of preemptive policing. Following a general trend of data-driven government that draws on self-learning algorithms and heterogeneous data sources, crime prediction software will likely be integrated into assemblages of predictive technologies where criminal events are indeed foreclosed before they can unfold and emerge, implying preemptive police action.

37. Ekaabi, M. A., Khalid, K., Davidson, R., Kamarudin, A. H., Preece, C. (2020), Smart policing service quality: conceptualisation, development and validation, Policing: An International Journal of Police Strategies and Management, 43, 5, 707-721. DOI: 10.1108/PIJPSM-03-2020-0038.

Abstract:

Purpose This study evaluates a multidimensional hierarchical scale of smart policing service quality. Design/methodology/approach Qualitative and quantitative analysis tools were used to develop a smart policing service quality scale based on the integrative psychometric scale development methodology. A multidimensional

hierarchical structure was proposed for smart policing service quality; a group of preliminary items selected from literature was used for the qualitative analysis. For data collection, users of smart policing services were selected through the United Arab Emirates (UAE) research centre. Several statistical methods were employed to verify reliability and validity of the construct and nomological validity of the proposed scale. Findings A smart policing service quality scale of 23 items was developed based on a hierarchical factor model structure. Nomological testing indicated that overall smart policing service quality is positive and significant, thus contributing to user satisfaction, intention to continue using the system and enhanced quality of life. Practical implications This study enables managers to evaluate types of policing quality and effectively implement strategies to address security and sustainability issues that exist currently in smart services. Originality/value Previous studies on policing service quality have not sufficiently addressed the role of smart policing service quality; the nature of discussion in this area is primarily based around concepts. The development of the smart policing service quality scale provides a measurement tool for researchers to use to enhance the understanding of smart policing service quality.

38. 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

Abstract

This article examines the impact of digital media technologies on police-lesbian, gay, bisexual, transgender, intersex and queer (LGBTIQ) community relations in Sydney

through a viral video of police excessive force filmed after the 2013 Sydney Gay and Lesbian Mardi Gras parade. Critical media analysis, and 15 in-depth interviews with police and non-police respondents directly affected by the video, make an in-depth, qualitative contribution to legitimacy and procedural justice studies on the impact of digital technologies on LGBTIQ community trust in police. The findings emphasise the capacity of amateur video of police excessive force publicised directly through social media to pressure the police to account, to catalyse LGBTIQ community responses and to negotiate through online fora legitimate boundaries of police practice. Exposure through social media can pressure the police to justify police transgression in real time; a form of 'dynamic' legitimacy requiring continuous and detailed justification of police practice that can exhaust standard police responses through a potentially infinite claim-response dialogue. Despite revision of policing practices at Mardi Gras since 2013, ongoing discrepancies between police understanding and public perceptions of a range of police tactics, including use of force, emphasise the continued importance of dialogue between police and LGBTIQ communities.

39. 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

Abstract

The effective, efficient and equitable policing of urban areas rests on an appreciation of the qualities and scale of, as well as the factors shaping, demand. It also requires an appreciation of the factors shaping the resources deployed in their address. To

this end, this article probes the extent to which policing demand (crime, anti-social behaviour, public safety and welfare) and deployment (front-line resource) are similarly conditioned by the social and physical urban environment, and by incident complexity. The prospect of exploring policing demand, deployment and their interplay is opened through the utilisation of big data and artificial intelligence and their integration with administrative and open data sources in a generalised method of moments (GMM) multilevel model. The research finds that policing demand and deployment hold varying and time-sensitive association with features of the urban environment. Moreover, we find that the complexities embedded in policing demands serve to shape both the cumulative and marginal resources expended in their address. Beyond their substantive policy relevance, these findings serve to open new avenues for urban criminological research centred on the consideration of the interplay between policing demand and deployment.

40. Enarsson, T., Enqvist, L., & Naarttijärvi, M. (2022) Approaching the human in the loop – legal perspectives on hybrid human/algorithmic decision-making in three contexts, *Information & Communications Technology Law*, 31,1, 123-153, DOI: 10.1080/13600834.2021.1958860

Abstract

Public and private organizations are increasingly implementing various algorithmic decision-making systems. Through legal and practical incentives, humans will often need to be kept in the loop of such decision-making to maintain human agency and accountability, provide legal safeguards, or perform quality control. Introducing such human oversight results in various forms of semi-automated, or hybrid decision-making - where algorithmic and human agents interact. Building on previous

research we illustrate the legal dependencies forming an impetus for hybrid decision-making in the policing, social welfare, and online moderation contexts. We highlight the further need to situate hybrid decision-making in a wider legal environment of data protection, constitutional and administrative legal principles, as well as the need for contextual analysis of such principles. Finally, we outline a research agenda to capture contextual legal dependencies of hybrid decision-making, pointing to the need to go beyond legal doctrinal studies by adopting socio-technical perspectives and empirical studies.

41. 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

Abstract

Police organizations internationally explore and experiment with new technologies to improve their performance and in response to new forms of crime. The police in the Netherlands experiment with various forms of innovative technology. Previous research has shown that social, organizational, and technological factors are important for effective use and deployment of technology by the police. However, the precise factors and mechanisms underlying the promotion or inhibition of technological innovations within the police are not clear. This study aims to provide empirical knowledge about these mechanisms by providing insight into the processes through which technological innovation develops within the police in the Netherlands. From January 2017 to February 2018, 13 technological innovation projects were subjected to a longitudinal process study. The results show that

innovation processes within the police organization are often inhibited by organizational factors, whereas social factors can stimulate and promote these processes.

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

Abstract

Automated facial recognition (AFR) has emerged as one of the most controversial policing innovations of recent years. Drawing on empirical data collected during the United Kingdom's two major police trials of AFR deployments—and building on insights from the sociology of policing, surveillance studies and science and technology studies—this article advances several arguments. Tracing a lineage from early sociologies of policing that accented the importance of police discretion and suspicion formation, the analysis illuminates how technological capability is conditioned by police discretion, but police discretion itself is also contingent on affordances brought by the operational and technical environment. These, in turn, frame and 'legitimate' subjects of a reinvented and digitally mediated 'bureaucratic suspicion'.

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

Abstract

This article analyses adoptions of innovative technology into police surveillance activities. Extending the nascent body of empirical research on digital policing, the

article draws on qualitative interview data of operational police uses of advanced surveillance technologies. Separate illustrative examples are drawn from social media intelligence gathering, digital forensics and covert online child sexual exploitation investigations. Here, surveillance governance mechanisms, often authored in the 'pre-digital' era, are deemed ill-fitting to the possibilities brought by new technologies. This generates new spaces of interpretation, where regulatory frameworks become renegotiated and reinterpreted, a process defined here as 'surveillance arbitration'. These deliberations are resolved in myriad ways, including perceived licence for extended surveillance and, conversely, more cautious approaches motivated by perceived exposure to regulatory sanction.

44. 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

Abstract

This paper examines the problems for police reputation, operational effectiveness and integrity of the criminal justice system that can arise from off-duty use of social media (SM) by police officers. It locates recent trends in SM use against the background of changes in information and communication practices in policing and the wider community. The concept of police indiscretion is used to explore those features of SM that facilitate and encourage disclosures as well as to, using a series of case studies, identify the harms that can arise. It is suggested that there is currently insufficient appreciation of how SM is impacting upon policing and that, in contrast to the impacts of previous new technologies, SM has the potential to

transform many policing practices more quickly and in a more wholesale fashion. Some suggestions for responding to this scenario are offered.

45. Gramagila, J.A., & Phillips, S.W. (2018). Police Officers' Perceptions of Body-Worn Cameras in Buffalo and Rochester. *American Journal of Criminal Justice* 43, 313–328 https://doi.org/10.1007/s12103-017-9403-9

Abstract

Police body-worn cameras have been advanced as a solution to disparate perceptions among the citizenry, public officials, community leaders, and the police themselves in the highly contested arena of police-citizen encounters. As with previous innovations in policing it is important that programs or policies developed for street-level application be planned in advance, and the opinions of police officers should be understood prior to implementation. This study provides survey responses from police officers in Buffalo and Rochester regarding their perceptions of body-worn cameras. Survey items were borrowed from prior research in Phoenix and Los Angeles. It also included items intended to measure the officer's opinions about examining camera images prior to writing a report, an issue that is the subject of some disagreement among policy makers. Findings suggest similar attitudes toward body cameras not only among Buffalo and Rochester police officers, but also with police officers in other agencies. Almost all respondents agree or strongly agree that police officers should have the ability to review body camera images prior to writing a report. The policy implications of this finding are discussed.

46. 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

Abstract

Based primarily on research into the policing of football fans in Scotland following the implementation of the Offensive Behaviour at Football and Threatening Communications Act (Scotland) Act 2012 this paper examines the interplay of police techniques and surveillance technologies in the policing of Scottish football. There has been relatively little academic attention directed towards the Act, so the question of why and how this flagship legislation generated such intense opposition that it was repealed within six years of its introduction demands investigation. This paper explores the implementation of the Act from the perspectives of football fans, criminal justice agencies, and representatives of football clubs, with a specific focus on the impact of police surveillance practices. The research uncovered strong perceptions that such practices were considered intimidatory, which may have weakened the perceived legitimacy of the Act. This paper poses a challenge to simple readings of evidence in terms of the claimed benefits of particular forms of surveillance, arguing that the use of technologies such as powerful hand-held cameras and body worn video (BWV) has had a detrimental impact on police-fan relationships, interactions and dialogue.

47. Harfield, C. (2021) Was Snowden virtuous?. *Ethics Inf Technol* 23, 373–383 https://doi.org/10.1007/s10676-021-09580-4

Abstract

Professor Shannon Vallor's theoretical framework of technomoral virtue ethics identifies character traits that can be cultivated to foster a future worth wanting in an environment of (mostly digital) emerging technologies. Such technologies and increased citizen participation in the new digital environment have reconfigured what is possible in policing and intelligence-gathering more quickly, perhaps, than sober and sensible policy reflection and formulation can keep pace with. Sensational and dramatic, seismic and devastating, the Snowden disclosures represent a particular expression of dissent against American intelligence community exploitation of emerging technologies in undertaking mass surveillance on a global scale. Responses to Snowden's actions, and perceptions of the (dis)value of the disclosures he made, are polarized. Polar opposites equate to vices in the Aristotlean view that posits virtue as the middle way. Here, the theoretical framework of technomoral virtue ethics is used for objective evaluation of Snowden's asserted motivations and documented actions against the benchmark of good cyber-citizenship that the framework describes. The fact that Snowden's account is strongly disputed by the U.S. Government does not in and of itself invalidate a theoretical evaluation. It is not the probative value of Snowden's account that is being tested, but how the narrative presented measures up to an ethical framework.

48. 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

Abstract

This article introduces the concept of Artificial Intelligence (AI) to a criminological audience. After a general review of the phenomenon (including brief explanations of important cognate fields such as ‘machine learning’, ‘deep learning’, and ‘reinforcement learning’), the paper then turns to the potential application of AI by criminals, including what we term here ‘crimes with AI’, ‘crimes against AI’, and ‘crimes by AI’. In these sections, our aim is to highlight AI’s potential as a criminogenic phenomenon, both in terms of scaling up existing crimes and facilitating new digital transgressions. In the third part of the article, we turn our attention to the main ways the AI paradigm is transforming policing, surveillance, and criminal justice practices via diffuse monitoring modalities based on prediction and prevention. Throughout the paper, we deploy an array of programmatic examples which, collectively, we hope will serve as a useful AI primer for criminologists interested in the ‘tech-crime nexus’.

49. Healey, K. and Stephens, N. (2017), Augmenting justice: Google glass, body cameras, and the politics of wearable technology, *Journal of Information, Communication and Ethics in Society*, 15, 4, 370-384. https://doi.org/10.1108/JICES-04-2016-0010

Abstract

Purpose: This paper aims to uncover the assumptions and concerns driving public debates about Google Glass and police body cameras. In doing so, it shows how debates about wearable cameras reflect broader cultural tensions surrounding race and privilege.

Design/methodology/approach: The paper employs a form of critical discourse analysis to discover patterns in journalistic coverage of these two technologies.
Findings: Public response to Glass has been overwhelmingly negative, while response to body cameras has been positive. Analysis indicates that this contrasting response reflects a consistent public concern about the dynamics of power and privilege in the digital economy. While this concern is well-founded, news coverage indicates that technologists, policy makers and citizens each hold assumptions about the inevitability and unvarnished beneficence of technology.
Research limitations/implications: Since this qualitative approach seeks to discern broad emergent patterns, it does not employ a quantifiable and reproducible coding schema.
Practical implications: The article concludes by arguing that grassroots action, appropriate regulatory policy and revitalized systems of professional journalism are indispensable as the struggle for social justice unfolds in the emerging digital economy.
Social implications: These debates represent a struggle over what and how people see. Yet public discourse often glosses over the disadvantages of technological change, which impacts who is able to amass social power.
Originality/value: This comparative approach yields unique conceptual insight into debates about technologies that augment ways of seeing.

50. 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

Abstract

Public demands for greater police accountability, particularly in relation to violence targeting Black and Brown communities, have placed pressure on law enforcement organisations to be more transparent about officers' actions. The implementation of police body-worn cameras (BWCs) has become a popular response. This article examines the embrace of BWCs amidst the wider shift toward evidence-based policing by scrutinising the body of research that evaluates the effects of these technologies. Through an intertextual analysis informed by insights from Critical Race Theory and Science and Technology Studies, we illustrate how the privileging of certain forms of empiricism, particularly randomised controlled trials, evinces what Woolgar and Pawluch describe as ontological gerrymandering. In doing so, the emergent evidence base supporting BWCs as a policing tool constitutively redefines police violence into a narrow conceptualisation rooted in encounters between citizens and police. This analysis examines how these framings, by design, minimise racialised power relations and inequalities. We conclude by reflecting on the implications of these evidence-based claims, arguing that they can direct attention away from – and thus can buttress – the structural conditions and institutions that perpetuate police violence.

51. 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

Abstract

Police departments across the United States are now integrating new visual monitoring technology (e.g. unmanned aerial vehicles [UAVs or'drones'], body

cameras) into routine police practices. Despite their potential use in multiple areas of proactive and reactive policing, public attitudes toward police use of UAVs, and visual monitoring technology overall, is mixed. As an extension of previous research, the current study uses a national survey to assess how well individuals' perceptions about police legitimacy, effectiveness, and other criminal justice attitudes predict the level of public receptivity and opposition toward police UAV use in various contexts. The implications of these findings for public policy and law enforcement practices are discussed.

52. 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

Abstract

Debates about effective responses to the COVID-19 pandemic have emphasized the paramount importance of digital tracing technology in suppressing the disease. So far, discussions about the ethics of this technology have focused on privacy concerns, efficacy, and uptake. However, important issues regarding power imbalances and vulnerability also warrant attention. As demonstrated in other forms of digital surveillance, vulnerable subpopulations pay a higher price for surveillance measures. There is reason to worry that some types of COVID-19 technology might lead to the employment of disproportionate profiling, policing, and criminalization of marginalized groups. It is, thus, of crucial importance to interrogate vulnerability in COVID-19 apps and ensure that the development, implementation, and data use of this surveillance technology avoids exacerbating vulnerability and the risk of harm to surveilled subpopulations, while maintaining the benefits of data collection across the

whole population. This paper outlines the major challenges and a set of values that should be taken into account when implementing disease surveillance technology in the pandemic response.

53. 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

Abstract

Police departments that emphasise certain strategic models (e.g. community-oriented policing, problem-oriented policing) may adopt specific types of technology to better achieve their core missions. A contrasting theory is that police agencies do not invest strategically in technology; rather, they adopt technology in a black box' without a larger plan for how a particular technology fits within the agency's guiding philosophy or operational goals. Despite the importance of this discourse, very little research has been conducted to address these claims. Using survey data from a large and nationally representative sample of police agencies in the United States (N=749), we examine whether strategic police goals are associated with technology use for six core technologies (crime mapping, social media, data mining software, car cameras, license plate readers (LPRs), and body-worn cameras (BWCs)). Nationally, across the sample of all US law enforcement agencies, we find little relationship between strategic goals and technology. Agency size, rather than policing philosophy was a more important determinant of technology use. However, stronger relationships between strategy and technology emerged when the analysis was limited to a subsample of larger agencies (250 or more sworn officers).

Specifically, community and hot spot policing strategies were positively associated with the use of geographic information system technology, social media, and LPRs. Agencies who emphasised hot spot policing were also more likely to have used BWCs. Implications of these findings are discussed.

54. Henman, P. (2019) Of algorithms, Apps and advice: digital social policy and service delivery, *Journal of Asian Public Policy*, 12, 1, 71-89, DOI: 10.1080/17516234.2018.1495885

Abstract:

Governments across the world have been developing and adopting new digital technologies for about a half of a century to support policy making and service delivery processes. Yet, until recently minimal critical attention has been given to this phenomenon and how it is transforming government. This paper reviews recent research on new and emerging technologies and the associated transformations they have for government policy and service delivery and the consequences for citizens and service users. The paper focuses on three key uses of digital technologies: automation, apps and advice. With the use of these examples, the paper demonstrates that visions of digital government of greater efficiency, improved quality of service delivery and open and accountable government are often not achieved. The paper concludes by acknowledging the ongoing importance of digital technologies in government, but also a need for a critical awareness of the power context of the adoption of technologies, of how policy and administrative principles may be undermined, and how populations may be increasingly segmented, fragmented and controlled.

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

Abstract

Objectives Test whether (1) people view a policing decision made by an algorithm as more or less trustworthy than when an officer makes the same decision; (2) people who are presented with a specific instance of algorithmic policing have greater or lesser support for the general use of algorithmic policing in general; and (3) people use trust as a heuristic through which to make sense of an unfamiliar technology like algorithmic policing. Methods An online experiment tested whether different decision-making methods, outcomes and scenario types affect judgements about the appropriateness and fairness of decision-making and the general acceptability of police use of this particular technology. Results People see a decision as less fair and less appropriate when an algorithm decides, compared to when an officer decides. Yet, perceptions of fairness and appropriateness were strong predictors of support for police use of algorithms, and being exposed to a successful use of an algorithm was linked, via trust in the decision made, to greater support for police use of algorithms. Conclusions Making decisions solely based on algorithms might damage trust, and the more police rely solely on algorithmic decision-making, the less trusting people may be in decisions. However, mere exposure to the successful use of algorithms seems to enhance the general acceptability of this technology.

55. 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.

Abstract

This paper explores the rapid deployment of police body-worn cameras (BWCs) and the subsequent push for the integration of biometric technologies (i.e., facial recognition) into these devices. To understand the political dangers of these technologies, I outline the concept of "making the body electric" to provide a critical language for cultural practices of identifying, augmenting, and fixing the body through technological means. Further, I argue how these practices reinforce normative understandings of the body and its political functionality, specifically with BWCs and facial recognition. I then analyze the rise of BWCs in a cultural moment of high-profile police violence against unarmed people of color in the United States. In addition to examining the ethics of BWCs, I examine the politics of facial recognition and the dangers that this form of biometric surveillance pose for marginalized groups, arguing against the interface of these two technologies. The pairing of BWCs with facial recognition presents a number of sociopolitical dangers that reinforce the privilege of perspective granted to police in visual understandings of law enforcement activity. It is the goal of this paper to advance critical discussion of BWCs and biometric surveillance as mechanisms for leveraging political power and racial marginalization.

56. 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.

Abstract

This review explores past and future shifts in policing and criminology scholarship that have shaped, and been shaped by, what is done to enhance safety within political domains. Investigating established policing conceptualizations, the review demonstrates how the ideal of state -delivered safety as a public good was challenged by a sizeable policing industry, giving rise to debates about legal context, service provision, and conceptualizations of policing and security nodal arrangements. This review argues that these understandings are now confronted by new harms and new conceptualizations of social institutional affairs. Interrogating these claims through an examination of the Anthropocene and technologies of cyberspace, we canvass debates and show that a shared focus of attention for the future of policing will be a decentralization of security and an expansion of private security governance professionals (both human and nonhuman).

57. Huff, J., Katz, C.M. & Webb, V.J. (2018), Understanding police officer resistance to body-worn cameras, *Policing: An International Journal*, 41, 4, 482-495. https://doi.org/10.1108/PIJPSM-03-2018-0038

Abstract

Purpose: Body-worn cameras (BWCs) have been adopted in police agencies across the USA in efforts to increase police transparency and accountability. This widespread implementation has occurred despite some notable resistance to BWCs

from police officers in some jurisdictions. This resistance poses a threat to the appropriate implementation of this technology and adherence to BWC policies. The purpose of this paper is to examine factors that could explain variation in officer receptivity to BWCs.

Design/methodology/approach: The authors assess differences between officers who volunteered to wear a BWC and officers who resisted wearing a BWC as part of a larger randomized controlled trial of BWCs in the Phoenix Police Department. The authors specifically examine whether officer educational attainment, prior use of a BWC, attitudes toward BWCs, perceptions of organizational justice, support for procedural justice, noble cause beliefs, and official measures of officer activity predict receptivity to BWCs among 125 officers using binary logistic regression.

Findings: The findings indicate limited differences between BWC volunteers and resistors. Volunteers did have higher levels of educational attainment and were more likely to agree that BWCs improve citizen behaviors, relative to their resistant counterparts. Interestingly, there were no differences in perceptions of organizational justice, self-initiated activities, use of force, or citizen complaints between these groups.

Originality/value: Though a growing body of research has examined the impact of BWCs on officer use of force and citizen complaints, less research has examined officer attitudes toward the adoption of this technology. Extant research in this area largely focusses on general perceptions of BWCs, as opposed to officer characteristics that could predict receptivity to BWCs. This paper addresses this limitation in the research.

58. Hunton P. (2011), A rigorous approach to formalising the technical investigation stages of cybercrime and criminality within a UK law enforcement environment, *Digital Investigation*, 7, 3-4, 105-113, https://doi.org/10.1016/j.diin.2011.01.002.

Abstract

As the Internet evolves and continues to become a compelling part of our everyday lives, individuals, communities and nations alike are becoming increasingly exposed to the growing threat of the cybercriminal. The aim of this paper is to widen the discussion surrounding the many global issues and challenges of cybercrime investigation with specific reference to UK law enforcement. This paper first discusses the vast transnational landscape now associated with cybercrime and the rapid growth in cyber offences and other unacceptable Internet behaviours. The emerging characteristics of cybercrime are then presented as a Cybercrime Execution Stack. This logical model of cybercrime demonstrates an objective view and is aimed at identifying the common characteristics of cyber criminality that are likely to occur during the commission of an offence or other illicit behaviours. The concepts of a cybercrime investigation framework focussing on a UK law enforcement environment are introduced following the stages of Initiation, Modelling, Assessment, Impact and Risks, Planning, Tools, Action and Outcome. The benefits of such a framework are intended to provide a cybercrime investigator with a much richer understanding of the complex technical elements of networked technology and the Internet that must be considered when conducting a rigorous cybercrime investigation.

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

Abstract

What will be the consequences for policing as cities become increasingly ‘smarter’? The emerging questions about policing and the smart city have thus far focused primarily on the increased surveillance capacity that a highly networked urban setting provides for law enforcement. More cameras and sensors will mean more watching and less freedom from being watched. The perception of ubiquitous government surveillance might quell dissent and inhibit free expression. As a result, concerns about policing and the smart city echo other responses to surveillance technologies. This essay proposes a different analysis: as cities become ‘smarter’, they increasingly embed policing itself into the urban infrastructure. Policing is inherent to the smart city.

60. 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

Abstract

Police professionals and practitioners offer reflections and commentary on the articles describing the Smart Policing Initiatives in Boston, Glendale, Los Angeles, and Lowell. According to the authors, police collaborations are vital to decision making regarding police policies and practices, yet they are not “natural.” Police–researcher collaborations require a conscious effort by both parties to overcome traditional organizational cultures and barriers to collaboration, and to establish, nurture, and maintain trust. The commentators also note the importance of

technology and sophisticated analytics, as well as the key role played by problem-solving in Smart Policing Initiatives; a process that, again, requires a strong, trustful research collaboration.

61. 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

Abstract

In R (on the application of Bridges) v Chief Constable of South Wales Police the Court of Appeal held the deployment of live automated facial recognition technology (AFR) by the South Wales Police Force (SWP) unlawful on three grounds. It violated the right to respect for private life under Article 8 of the European Convention on Human Rights because it lacked a suitable basis in law; the Data Protection Impact Assessment carried out under section 64 of the Data Protection Act 2018 was deficient for failing to assess the risks to the rights and freedoms of individuals processed by the system; and SWP failed to fulfil the Public Service Equality Duty imposed by section 149 of the Equality Act 2010 by failing to assess whether or not the software used in the AFR system was biased in relation to sex and race.

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

Abstract

This article explores in empirical detail the air-bound expectations, imaginations and practices arising from the acquisition of a new police drone in the Swiss canton of Neuchâtel. The study shows how drones are transforming the ways in which the

aerial realm is lived as a context, object and perspective of policing. This tripartite structure is taken as a prism through which to advance novel understandings of the simultaneously elemental and affective, sensory, cognitive and practical dimensions of the aerial volumes within, on and through which drones act. The study of the ways in which these differing dimensions are bound together in how the police think about drones and what they do with them enables the development of an 'aerial geopolitics of security' that, from a security viewpoint, approaches interactions between power and space in a three-dimensional and cross-ontological way.

63. Gaelle, K. & Joëlle, V., (2018), How Could the Ethical Management of Health Data in the Medical Field Inform Police Use of DNA? *Frontiers in Public Health*, DOI=10.3389/fpubh.2018.00154

Abstract

Various events paved the way for the production of ethical norms regulating biomedical practices, from the Nuremberg Code (1947) —produced by the international trial of Nazi regime leaders and collaborators—and the Declaration of Helsinki by the World Medical Association (1964) to the invention of the term "bioethics" by American biologist (1). The ethics of biomedicine has given rise to various controversies—particularly in the fields of newborn screening (2), prenatal screening (3), and cloning (4)—resulting in the institutionalization of ethical questions in the biomedical world of genetics. In 1994, France passed legislation—commonly known as the "bioethics laws"— to regulate medical practices in genetics. The medical community has also organized itself in order to manage ethical issues relating to its decisions, with a view to handling "practices with many strong uncertainties" and enabling clinical judgments and decisions to be taken not by

individual practitioners but rather by multidisciplinary groups drawing on different modes of judgment and forms of expertise (5). Thus, the biomedical approach to genetics has been characterized by various debates and the existence of public controversies. In the judicial sphere, the situation is very different. Since the end of the 1990s, developments in biomedical research have led to genetic data being used in police work and legal proceedings. Today, the forensic police are omnipresent in investigations: not just in complex criminal cases but also routinely in cases of “minor” or “mass” delinquency. Genetics, which certainly receives the most media coverage among the techniques involved (6), has taken on considerable importance (7). However, although very similar techniques are used in biomedicine and police work (DNA amplification, sequencing, etc.), the forms of collective management surrounding them are very different, as well as the ethico-legal frameworks and their evolution, as this text will demonstrate.

64. 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

Abstract

Technology is often highlighted in popular discourse as a causal factor in significantly increasing sex trafficking. However, there is a paucity of robust empirical evidence on sex trafficking and the extent to which technology facilitates it. This has not prevented the proliferation of beliefs that technology is essential for disrupting or even ending sex trafficking. Big data analytics and anti-trafficking software are used in this context to produce knowledge and intelligence on sex trafficking. This paper explores the challenges and limitations of understanding exploitation through

algorithms and online data. It also highlights the key dimensions of exploitation ignored in big data-oriented research on sex trafficking. By doing so, the paper seeks to advance our theoretical understanding of the trafficking–technology nexus, and it is argued that sex trafficking must be reframed along a continuum of exploitation that is sensitive to the social context of exploitation within the sex market.

65. 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.

Abstract

Background: Recent technological advances have much potential for improving police performance, but there has been little research testing whether they have made police more effective in reducing crime.

Objective: To study the uses and crime control impacts of mobile computing technology in the context of geographically focused “hot spots” patrols.

Research Design: An experiment was conducted using 18 crime hot spots in a suburban jurisdiction. Nine of these locations were randomly selected to receive additional patrols over 11 weeks. Researchers studied officers’ use of mobile information technology (IT) during the patrols using activity logs and interviews. Nonrandomized subgroup and multivariate analyses were employed to determine if and how the effects of the patrols varied based on these patterns.

Results: Officers used mobile computing technology primarily for surveillance and enforcement (e.g., checking automobile license plates and running checks on people during traffic stops and field interviews), and they noted both advantages and disadvantages to its use. Officers did not often use technology for strategic problem-

solving and crime prevention. Given sufficient (but modest) dosages, the extra patrols reduced crime at the hot spots, but this effect was smaller in places where officers made greater use of technology.

Conclusions: Basic applications of mobile computing may have little if any direct, measurable impact on officers' ability to reduce crime in the field. Greater training and emphasis on strategic uses of IT for problem-solving and crime prevention, and greater attention to its behavioral effects on officers, might enhance its application for crime reduction.

66. Koziarski, J. and Lee, J.R. (2020), Connecting evidence-based policing and cybercrime, *Policing: An International Journal*, 43, 1, 198-211. https://doi.org/10.1108/PIJPSM-07-2019-0107

Abstract

Purpose: This paper explores the various challenges associated with policing cybercrime, arguing that a failure to improve law enforcement responses to cybercrime may negatively impact their institutional legitimacy as reliable first responders. Further, the paper makes preliminary links between cybercrime and the paradigm of evidence-based policing (EBP), providing suggestions on how the paradigm can assist, develop, and improve a myriad of factors associated with policing cybercrime.

Design/methodology/approach: Three examples of prominent cybercrime incidents will be explored under the lens of institutional theory: the cyberextortion of Amanda Todd; the hacking of Ashley Madison; and the 2013 Target data breach.

Findings: EBP approaches to cybercrime can improve the effectiveness of existing and future approaches to cybercrime training, recruitment, as well as officers' preparedness and awareness of cybercrime.
Research limitations/implications: Future research will benefit from determining what types of training work at the local, state/provincial, and federal level, as well as evaluating both current and new cybercrime policing programs and strategies.
Practical implications: EBP approaches to cybercrime have the potential to improve police responses to cybercrime calls for service, save police resources, improve police–public relations during calls for service, and improve police legitimacy.
Originality/value: This paper links cybercrime policing to the paradigm of EBP, highlighting the need for evaluating and implementing effective evidence-based approaches to policing cybercrime.

67. Kuo, P. F., & Lord, D., (2019), A promising example of smart policing: A cross-national study of the effectiveness of a data-driven approach to crime and traffic safety, *Case studies on Transport Policy*, 7, 4, 761-771. DOI: 10.1016/j.cstp.2019.08.005

Abstract:
Smart policing emphasizes the combination of existing interdisciplinary datasets, improvement in analysis procedures, and design of more efficient policing strategies. One promising example, the Data-Driven Approach to Crime and Traffic Safety (DDACTS), integrates traffic crash and crime data into the design of more efficient patrol routes, ensuring higher visibility traffic enforcement. This new method allows the police to more effectively allocate their limited resources. Although the DDACTS model has significantly reduced crime and crash rates in the United States, it is

necessary to thoroughly study its effects before applying it in other parts of the world; the factors that influence crime, crashes, and police patrol systems in the United States may differ significantly from those in, for instance, Asia. In the present research, Taiwan was chosen as an initial area of study because of the nation's open data policy and good quality of the data available. This study focused on two key differences between the United States and Taiwan: (1) the cluster distributions of crash and crime events, and (2) possible effectiveness of DDACTS in these two regions. ArcGIS was used to calculate point cluster patterns and identify hotspots. Although the point patterns for crimes and crashes varied greatly between Texas and Taiwan, all pairs of crash and crime hotspots were in close proximity to one another. Thus, DDACTS may be effective for improving patrol efficiency in Taiwan, despite the nation's significant socioeconomic differences with the United States Consequently, the results show that DDACTS may be efficient in various regions with different socioeconomic structures than the United States, such as countries in Asia. In the future, researchers from other nations may be able to use these results to revise and adjust their own DDACTS patrol plans.

68. L'Hoiry, X., Moretti, A. & Antonopoulos, G.A. (2021), Identifying sex trafficking in Adult Services Websites: an exploratory study with a British police force. *Trends Organ Crim*. https://doi.org/10.1007/s12117-021-09414-1

Abstract

Human trafficking, commercial sexual exploitation and modern slavery have experienced an unprecedented boom over the past decade due to the development of information and communication technologies (ICTs), particularly in digital and networked environments. These developments have created new opportunities for

human exploitation and illegal profiteering. Adult Services Websites (ASWs), online platforms on which sex workers post profiles advertising their services, are a key conduit for human traffickers to exploit their victims. Alongside profiles of independent sex workers, traffickers are posting false ASW profiles, advertising the forced services of their victims and camouflaging these false profiles amongst legitimate adverts. In response, police practitioners are proactively investigating ASWs to identify suspect profiles. A key obstacle for practitioners, however, is to distinguish between ASW profiles posted by independent, consenting sex workers advertising their services, and those posted by traffickers exploiting their victims. The exploratory study presented in this paper seeks to address this particular challenge. Working with a British police force, the researchers in this study gathered existing knowledge on the traffickers' use of ASW profiles to create a bespoke tool of analysis, the Sexual Trafficking Identification Matrix (STIM). The aim of this tool has been to identify 'risk indicators' on ASW profiles and to flag these for potential police investigation. This paper presents the results of this exploratory study and its four stages. Furthermore, more broadly, it reflects on the use of evidence-based tools by law enforcement to tackle complex domains of offending such as those of human trafficking and commercial sexual exploitation.

69. 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

Abstract

Digital technology now plays a critical role in policing and security management, with policing apps, drones and body-worn cameras potentially being game-changers. Adoption of such technologies is, however, not straightforward and depends upon the buy-in of senior management teams and users. This study examines what obstacles practitioners face in the procurement, deployment and use of crime prevention and detection technologies. The issue is explored through a number of expert interviews conducted with practitioners in London between August 2019 and March 2020. This work expands previous, more theoretical, literature on the topic by adding a practical perspective and advances the understanding of issues faced in innovation processes and their management. We identified a variety of issues and obstacles to technological innovation for policing. These include the deployment of new systems at the cost of old ones, lack of financial and political support, issues in public–private partnerships, and public acceptability. Although individual practitioners may have the expertise and willingness to unleash the full potential of surveillance and crime-reduction technologies, they are usually restrained by institutional rules or, in some cases, inefficiencies. In terms of the latter, this study especially highlights the negative impact of a lack of technical interoperability of different systems, missing inter- and intra-agency communication, and unclear guidelines and procedures.

70. Lindsay, R., Jackson, W., & Cooke, L. (2014) Empirical evaluation of a technology acceptance model for mobile policing, *Police Practice and Research*, 15, 5, 419-436, DOI: 10.1080/15614263.2013.829602

Abstract

Technology acceptance in policing is under-researched, yet mobile devices are widely implemented across UK police forces. The paper validates a mobile technology acceptance model (M-TAM) developed in a single police force. It shows that the M-TAM is transferrable to other UK police forces, and potentially worldwide. The influence of local supervision and fit of technology to roles and tasks are shown to be the most influential factors. Factors beyond the technology itself, such as the influence of peers and involvement of operational officers in technology investment decisions, must be considered to accommodate the strong cultural barriers in policing.

71. Lum, C., Koper, C. S., & Willis, J. (2017). Understanding the Limits of Technology's Impact on Police Effectiveness. *Police Quarterly*, 20, 2, 135–163. https://doi.org/10.1177/1098611116667279

Abstract

Technology has become a major source of expenditure and innovation in law enforcement and is assumed to hold great potential for enhancing police work. But does technology achieve these expectations? The current state of research on technology in policing is unclear about the links between technologies and outcomes such as work efficiencies, effectiveness in crime control, or improved police–community relationships. In this article, we present findings from a mixed-methods, multiagency study that examines factors that may mediate the connection between

technology adoption and outcome effectiveness in policing. We find that police view technology through technological and organizational frames determined by traditional and reactive policing approaches. These frames may limit technology's potential in the current reform era and cause unintended consequences.

72. 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

Abstract

In this article, we provide the most comprehensive narrative review to date of the research evidence base for body-worn cameras (BWCs). Seventy empirical studies of BWCs were examined covering the impact of cameras on officer behavior, officer perceptions, citizen behavior, citizen perceptions, police investigations, and police organizations. Although officers and citizens are generally supportive of BWC use, BWCs have not had statistically significant or consistent effects on most measures of officer and citizen behavior or citizens' views of police. Expectations and concerns surrounding BWCs among police leaders and citizens have not yet been realized by and large in the ways anticipated by each. Additionally, despite the large growth in BWC research, there continues to be a lacuna of knowledge on the impact that BWCs have on police organizations and police–citizen relationships more generally. Policy Implications - Regardless of the evidence-base, BWCs have already rapidly diffused into law enforcement, and many agencies will continue to adopt them. Policy implications from available evidence are not clear-cut, but most likely BWCs will not be an easy panacea for improving police performance, accountability, and relationships with citizens. To maximize the positive impacts of BWCs, police and

researchers will need to give more attention to the ways and contexts (organizational and community) in which BWCs are most beneficial or harmful. They will also need to address how BWCs can be used in police training, management, and internal investigations to achieve more fundamental organizational changes with the long-term potential to improve police performance, accountability, and legitimacy in the community.

73. Lumsden, K. (2013) Policing the roads: traffic cops, ‘Boy Racers’ and anti-social behaviour, *Policing and Society*, 23, 2, 204-221, DOI: 10.1080/10439463.2012.696642

Abstract

This article explores the policing and regulation of young motorists known in the United Kingdom as boy racers'. It demonstrates how police officers' definitional decisions in relation to driving behaviours were influenced by a range of exogenous and endogenous factors, which subsequently shaped the landscape of enforcement and interactions with the community and drivers. A shift over time in the nature of the problem due to urban regeneration, innovations in the technology of the motor car and the availability of anti-social behaviour legislation impacted upon the policing of urban space. The strategies employed in order to police the culture and the related urban space were reminiscent of a deeper policing tradition wherein managing incivilities and local problems is part of the community policing perspective. Data is presented from semi-structured interviews with police, residents and boy racers', and ethnographic fieldwork with the drivers in the city of Aberdeen, Scotland.

74. 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

Abstract

Police organisations have been slow with regards to the integration of services which are accessible and responsive to the needs of D/deaf citizens. This qualitative study explored the barriers which D/deaf citizens face when accessing police. It considered the impact of police initiatives designed to widen the avenues through which D/deaf people can contact them including information and communication technologies (i.e. Emergency SMS Text Services and Video Relay Services) and interpreters. The study involved focus groups with D/deaf citizens, interviews with police officers, and a review of police practices in England. The findings focus on cultural, technological and interactional barriers, and demonstrate that despite indications that members of this community are likely to be vulnerable in terms of victimisation, current policies, procedures and training do not address access requirements. Points of interest This article looks at the barriers faced by D/deaf citizens when accessing police services. Age, ethnicity and disability impacted on D/deaf citizens' access to services and their use of technologies to contact the police. D/deaf citizens felt that more work needed to be done to raise greater deaf awareness amongst police officers and to avoid misunderstandings. Some improvements in police service provision have been made, but a better engagement strategy is needed to build D/deaf citizens' confidence in the police. The research recommends that when designing police services and technologies, the focus must include the needs of D/deaf citizens.

75. Lumsden, K., & Goode, J. (2018). Policing Research and the Rise of the 'Evidence-Base': Police Officer and Staff Understandings of Research, its Implementation and 'What Works.' *Sociology,* 52, 4, 813–829. https://doi.org/10.1177/0038038516664684

Abstract

Despite the pitfalls identified in previous critiques of the evidence-based practice movement in education, health, medicine and social care, recent years have witnessed its spread to the realm of policing. This article considers the rise of evidence-based policy and practice as a dominant discourse in policing in the UK, and the implications this has for social scientists conducting research in this area, and for police officers and staff. Social scientists conducting research with police must consider organisational factors impacting upon police work, as well as the wider political agendas which constrain it – in this case, the ways in which the adoption of evidence-based policing and the related 'gold standard' used to evaluate research act as a 'technology of power' to shape the nature of policing/research. The discussion draws on semi-structured interviews conducted with police officers and staff from police forces in England.

76. Mastrobuoni, G., (2020), Crime is Terribly Revealing: Information Technology and Police Productivity, *The Review of Economic Studies*, 87, 6, 2727–2753, https://doi.org/10.1093/restud/rdaa009

Abstract

An increasing number of police departments use information technology (IT) to optimize patrolling strategies, yet little is known about its effectiveness in preventing crime. Based on quasi-random access to "predictive policing," this study shows that

IT improves police productivity as measured by crime clearance rates. Thanks to detailed information on individual incidents and offender-level identifiers it also shows that criminals strategies are predictable. Moreover, the introduction of predictive policing coincides with a large negative trend-discontinuity in crime rates. The benefit–cost ratio of this IT innovation appears to be large.

77. 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

Abstract

Though there has always been a close relationship between professional policing and technology, the sheer scale of operational dependence upon new technologies has begun to raise a number of concerns. In this paper I trace 3 kinds of contrasting dynamics in the perception of the policing/technology relationship. A first view has tended to see this relationship in largely unproblematic, positive terms, one which generally results in 'more efficient', cost-effective forms of policing. Against this, a more sceptical position can also be traced. On this view, whilst enhanced access to technology often benefits police performance, it has often also come with enhanced opportunities for misuse which threaten dystopian scenarios of coercion, denial of rights and - at worst - the spectre of technologised police states. I argue that a third view is now plausible, one that has been far less discussed, even though it may present the greatest challenge to the viability of policing as we have known it. For the emergent technologies now reshaping policing often involve automated tools like predictive algorithms or facial recognition systems. This raises the question of what

limits to the automation of policing there may be and whether automation will ultimately entail the 'end' of professional police forces as once envisioned by Peel.

78. 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.

Abstract

Within a short timeframe, social media have become to be widely used in government organizations. Social media gurus assume that the transformational capacities of social media result in similar communication strategies in different organizations. According to them, government is transforming into a user-generated state. This paper investigates this claim empirically by testing the claim of convergence in social media practices in three North-American police departments (Boston, Washington DC and Toronto). The research shows that the social media strategies are widely different: the Boston Police Department has developed a ‘push strategy’ while the Metropolitan Police Department in DC has developed a ‘push and pull strategy and the Toronto Police Service a ‘networking strategy’. The paper concludes that a combination of contextual and path-dependency factors accounts for differences in the emerging social media strategies of government organizations. Social media have a logic of their own but this logic only manifests itself if it lands on fertile soil in a government bureaucracy.

79. Merola, L. M., & Lum, C. (2014) Predicting public support for the use of license plate recognition technology by police, *Police Practice and Research*, 15, 5, 373-388, DOI: 10.1080/15614263.2013.814906

Abstract

The use of license plate recognition technology (LPR) by police is becoming increasingly common. LPR may be used for many purposes, ranging from stolen vehicle enforcement to more complex surveillance and predictive functions. Existing research does not examine community support for this technology, despite its potential to impact police legitimacy. Results from the first community LPR survey are presented and multinomial logistic regression models of citizen support for the technology are developed. Regression results suggest that a number of factors significantly predict citizen support for LPR use, including increased trust in police and the belief that LPR information is public information.

80. 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

Abstract

As unmanned aerial systems grow in popularity, police agencies are using this technology to provide aerial support for officers; however, public opinion could affect the success of this technological collaboration. Using social identity theory, researchers may be able to predict people's support for various government projects. In a series of studies, participants were presented with a brief description of a proposal for using police drones to monitor political protests. Additional information

was provided about the type of protest and type of person attending the protest. In general, conservatives were more supportive of police drones monitoring protests compared to liberals. However, this support was moderated by the type of participant and the type of protest; that is, support dropped when a participant believed that the protest supported their own political party beliefs. The current study provides a foundation for understanding what factors affect the public's support of police incorporating drones into their daily workforce in the US.

81. 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

Abstract

The body-worn camera (BWC), an audio and video recording device, has been increasingly adopted by law enforcement across the globe. Drawing on a qualitative study, this paper will explore the use of these mobile devices in the UK and examine the challenges that have been faced during its implementation in two British police forces. In particular, we will discuss how these cameras move with the police officer's bodily movements (both intentionally and unintentionally) and are used for policing purposes in different settings (such as urban and rural contexts or different operational units). Based on a set of semi-structured interviews with 26 police officers, this article will explore the contextual, technical and ethical challenges that hinder the use of BWCs in such settings. This study concludes that these practical and techno-social challenges are often interlinked. The context of use of these cameras and how they operate technically are connected, often raising significant ethical issues particularly for data management and storage. Ultimately it is argued

that the operational perspective of the frontline officer is invaluable when designing and implementing technologies so they are policeman-proof.

82. Moon, H., Choi, H., Lee, J., & Lee, K. S. (2017), Attitudes in Korea toward Introducing Smart Policing Technologies: Differences between the General Public and Police Officers. *Sustainability,* 9, 10, 1921. https://doi.org/10.3390/su9101921

Abstract

This study analyzes different attitudes toward introduction of smart policing technologies in cybercrime policing among the Korean public and police. Policing is essential for a sustainable community. Technological advances in policing have both positive and negative aspects, making it essential to investigate perceptions of both public and police when introducing smart policing technologies. A discrete choice experiment was undertaken to survey preferences of the public and police toward introduction of such technologies and conduct simulation analysis to compare changes in the acceptance of various scenarios. The study divides cybercrime policing into prevention and investigation. The sample included 500 members of the public and 161 police officers. The results show that the public thinks an increase in yearly taxes and invasion of privacy are the most important factors. Conversely, the police think factors enhancing the efficiency of policing are most important. Moreover, when smart policing technologies are introduced, the public and police perceive more utility in the prevention and investigation of cybercrime, respectively. Few studies in this field separate the prevention and investigation of crimes, or compare perceptions of the public and police toward the introduction of smart

policing technologies. This study's quantitative analysis provides insights lacking in previous literature.

83. Mugari, I., & Obioha, E. E. (2021), Predictive Policing and Crime Control in The United States of America and Europe: Trends in a Decade of Research and the Future of Predictive Policing. *Social Sciences*, 10, 6, 234. https://doi.org/10.3390/socsci10060234

Abstract

There has been a significant focus on predictive policing systems, as law enforcement agents embrace modern technology to forecast criminal activity. Most developed nations have implemented predictive policing, albeit with mixed reactions over its effectiveness. Whilst at its inception, predictive policing involved simple heuristics and algorithms, it has increased in sophistication in the ever-changing technological environment. This paper, which is based on a literature survey, examines predictive policing over the last decade (2010 to 2020). The paper examines how various nations have implemented predictive policing and also documents the impediments to predictive policing. The paper reveals that despite the adoption of predictive software applications such as PredPol, Risk Terrain Modelling, HunchLab, PreMap, PRECOBS, Crime Anticipation System, and Azevea, there are several impediments that have militated against the effectiveness of predictive policing, and these include low predictive accuracy, limited scope of crimes that can be predicted, high cost of predictive policing software, flawed data input, and the biased nature of some predictive software applications. Despite these challenges, the paper reveals that there is consensus by the majority of the researchers on the importance of predictive algorithms on the policing landscape.

84. 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

Abstract

Body-worn cameras are increasingly being used by police forces and other government agencies across Australia to record interactions with suspects, witnesses and other members of the public. The cameras are thought to be capable of deterring officer misconduct, improving civilian behaviour and capturing valuable evidence of criminal wrongdoing. Unfortunately, in Australia, little public or academic attention has been directed to the privacy implications of these devices. This is in contrast to the United States, where there is vigorous debate about the potential for body-worn cameras to intrude upon the privacy of vulnerable individuals and to contribute to the over-surveillance of minority communities. One promising response to privacy concerns in the United States has been to democratise the rules around body-worn cameras by involving the public in the formulation of police guidelines. This Comment suggests that Australia should similarly involve the public in body-worn camera policy formulation.

85. O'Brien, M. (2009) Still on the road? Technology and historical perspectives on counter-cultural policing, *Information & Communications Technology Law*, 18, 3, 285-296, DOI: 10.1080/13600830903424726

Abstract

Technological development in the last 20 years has had a significant input into what is policed and how such policing takes place. This article seeks to explore the

policing of a part of the counter-culture in the United Kingdom, the so-called 'New Age Traveller', and in doing so highlight the impact of technology in relation to public order control.

86. 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

Abstract

As the first of its kind in UK policing, the West Midlands Police and Crime Commissioner and West Midlands Police data ethics committee is an ongoing experiment in scrutinising and advising upon AI policing projects proposed for real operational environments, with the aim of putting people's rights at the heart of technological development. Using a qualitative action research approach akin to an 'observing participant', this paper suggests that lessons can be learned from the committee's activities in three main areas: i) the contribution to effective accountability in respect of ongoing data analytics projects; ii) the importance of the legal and scientific aspects of the interdisciplinary analysis; and iii) the role of necessity and the human rights framework in guiding the committee's ethical discussion.

87. Nichols, J.,Wire, S., Wu, X., Sloan, M., & Scherer, A. (2019) Translational criminology and its importance in policing: a review, *Police Practice and Research*, 20, 6, 537-551, DOI: 10.1080/15614263.2019.1657625

Abstract

Translational criminology is a decision-making perspective that emphasizes the dynamic coproduction of evidence by researchers and practitioners, focusing on obstacles to and facilitators of evidence generation and utilization. It incorporates several other data-driven decision-making models, including evidence-based policy making. This review suggests that the availability of empirical research is no longer the most significant impediment to evidence-based policing. Rather, translating and implementing knowledge about 'what works' in policing has arisen as the field's primary barrier to securing the effectiveness and efficiency improvements of research and data utilization. This article orients readers to translational criminology's various components and explores their applications. Focusing on four central considerations, this review explores the roles of researcher practitioner partnerships, policy, technology, and government in developing and sustaining translational efforts in policing. The review concludes by acknowledging challenges to fostering a translational perspective in policing, and offers examples of where it has been applied with success.

88. 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

Abstract

Big Data is seen as an increasingly important tool to support policing activities, define security governance policies and assist criminal investigations. Although significant literature has explored the predictive capabilities of Big Data, there has been less focus on the uses of Big Data in criminal investigations, focused on detection and apprehension that occur after a crime has been committed. This article aims to fill this gap through the lens of expectations of professionals involved in police cooperation in the European Union. Based upon a set of qualitative interviews, our analysis explores these professionals' expectations for the application of Big Data techniques in criminal investigations by using DNA data held in national criminal DNA databases and, therefore, potentially increasing the interoperability between genetic and non-genetic data. Our results reveal a flexible repertoire of interpretation of the expectations for the uses of Big Data in criminal investigations and its associated potential risks and benefits. The perceived benefits relate to expectations for Big Data's potential to advance cold cases and strengthen the interoperability of multiple datasets in ways that produce intelligence valuable for criminal investigations. Perceived risks concern the difficulties associated with investigating large sets of data, the potential for enforcing genetic discrimination, and threatening privacy and human rights.

89. 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

Abstract:

England and Wales is currently privatizing most of its Probation Service and simultaneously planning to create the largest and most advanced electronic

monitoring (EM) scheme in the world, using combined GPS tracking and radio frequency technology. Downgrading one, upgrading the other. Using a mix of published and unpublished sources, discussions with some key players in these developments, (and a 'critical policy analysis' perspective), this article begins by documenting the post-2010 development of GPS tracking, and the emergence of strong police support for its large-scale use. It notes the role of a right-wing think tank, Policy Exchange, in promoting the view that the GPS-based tracking of offenders' movements is an intrinsically superior form of 'electronic monitoring' that should fully replace the discredited but still prevailing radio frequency EM, which can only restrict people to a single location. In the course of devising a third contract with commercial organizations to deliver EM, it transpired that the incumbent providers had been systematically overcharging the government for their services. Although a public scandal, and a series of official enquires - summarized here - resulted from this, the general momentum behind the outsourcing of penal interventions has not been slowed: the Conservative-led Coalition government is pursuing a relentlessly neoliberal agenda, driven far more by financial imperatives and technological preferences than anything that makes proper penal sense. The creation of a large, advanced GPS-based EM programme may not in fact work out in practice, but the government's readiness to envision it shows where untrammelled neoliberalism points in respect of 'offender management' techniques. Although England and Wales have always been anomalous in their fully privatized delivery of EM, its preparedness to invest massively in GPS tracking and to simultaneously sacrifice the state-based Probation Service should serve to warn other European services of the penal challenges that neoliberalism may present them with.

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

Abstract

In this article, Peter Neyroud, Chief Executive of the NPIA, and Emma Disley, DPhil student at the Centre for Criminology, University of Oxford, argue that factual questions about the effectiveness of new technologies (such as DNA evidence, mobile identification technologies and computer databases) in detecting and preventing crime should not, and cannot, be separated from ethical and social questions surrounding the impact which these technologies might have upon civil liberties. This is due to the close inter-relationship between the effectiveness of the police and public perceptions of police legitimacy—which may potentially be damaged if new technologies are not deployed carefully. The authors argue that strong, transparent management and oversight of these technologies are essential, and suggest some factors to which a regime of governance should attend.

91. 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.

Abstract

Research presented in this study examines the potentiality of artificial intelligence as an interrogator within a police interrogation to promote a non-biased environment in an effort to mitigate the ongoing racial and gender divide in statistics regarding false confessions. Ideally, artificial intelligence supplementation may help promote the

elicitation of non-coerced, voluntary confessions. This study suggests that the racial and gender bias influencing false confessions may be due to the two fold bias occurring within the interrogator-to-suspect dynamic, referenced in this study as “the Bias-Uncooperative Loop.” It argues that applying artificial intelligence within the interrogation room may minimize the two fold bias occurring in the dynamic. It suggests the potential for cooperation between the two parties can be conditioned by programmable similarity; whereby artificial intelligence can mimic the racial, ethnic and/or cultural similarities of the suspect in question. This is reflected in research in different arenas (not inclusive to interrogations) to have an effect on enhanced comfortability and cooperation with AI. This paper assumes similar results within interrogations.

92. 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

Abstract

Technology has always played an important role in policing. In recent years, various types of new social networking sites have become important tools for police departments. For example, social networking sites have been used to help solve crimes and communicate directly with the public circumventing the traditional news media. At the same time, the public can more easily communicate directly with, or about, the police. This article examines the use of Twitter by police departments on an everyday basis. Drawing on a content analysis of Canadian police departments' Twitter accounts, this article discusses the types of information sent out to the public (i.e. on crimes/investigations, police work, safety/traffic, and community) as well as

police attempts to interact with citizens (i.e. through invitations to attend events, asking for responses, and responding to and/or mentioning others). The findings suggest that Twitter was used to help manage the image of the police and build community. The implications of these findings are also discussed.

93. Oh, G., Zhang, Y., & Greenleaf, R. G. (2021). Measuring Geographic Sentiment toward Police Using Social Media Data. *American Journal of Criminal Justice*, https://doi.org/10.1007/s12103-021-09614-z

Abstract

Using Twitter messages published online from October 2018 to June 2019, and opinion mining (OM) technology, the current study analyzes the geographic sentiments toward police in 82 metropolitan areas within the United States. Building on the frameworks of the neighborhood social contextual models, the construct validity of “sentiment toward the police” is assessed via its relationship with the features of various metropolitan areas. Results of the regression analysis indicate that the violent crime rate, racial heterogeneity, and economic disadvantage significantly affect sentiment toward the police. Our results suggest that opinion mining of social media can be an important instrument to understand public sentiment toward the police.

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

Abstract

Over the past decade, U.S. police departments have incorporated media technologies that promise to make policing more efficient and "race-neutral," including body and dash cameras, drones, and predictive analytics. Such tools are positioned as unbiased and therefore reliable instruments that will hold both the state and citizens accountable during police interactions. This neutrality occurs along axes of race and affect, and presumes these technologies as anti-emotional third-party witnesses to exchanges between the state and public. In this article, we connect the expansion of high-tech policing to the racialized and gendered management of affect, underscoring how the supposed accountability offered by these technologies does not upend the disciplining of emotion. We examine the relationship between affective governance and media technologies through an analysis of Diamond Reynolds' Facebook Live video of police killing her boyfriend Philando Castile, which we theorize alongside the dash camera video of Sandra Bland, a 28-year-old Black woman who was pulled over by a police officer and arrested, and who allegedly died by suicide in jail three days later. We argue that taken together, the videos demonstrate the ongoing racialized and gendered imperative that Black women regulate their emotional reactions to state violence both despite and because of the presence of recording devices.

95. Parmar, A. (2019). Policing Migration and Racial Technologies, *The British Journal of Criminology*, 59, 4, 938–957, https://doi.org/10.1093/bjc/azz006

Abstract

The merger between familiar modes of policing with the impetus for migration control is reorganizing the racial politics of policing in unexpected ways. In the aim to decipher who is a citizen, who is a foreign national offender and who is eligible for deportation on the grounds of criminality, the role of criminal records agencies has expanded further into the work of policing, as have the collaborative working partnerships between immigration and the police. In this article, I discuss the findings from research, which examines the policing of migration in the United Kingdom, and specifically Operation Nexus, which brings together ordinary police work and migration control. I focus on how technologies of border control are imbricated with everyday police practices that are often influenced by race, thereby deepening the reach of racial technologies and their capacity to monitor and exclude racial others.

96. Parry, M. M. Moule, R. K., & Dario, L. M. (2019) Technology-Mediated Exposure to Police–Citizen Encounters: A Quasi-Experimental Assessment of Consequences for Citizen Perceptions, *Justice Quarterly*, 36, 3, 412-436, DOI: 10.1080/07418825.2017.1374435

Abstract

Anecdotal evidence suggests that recent video-recorded police-citizen encounters have undermined police legitimacy and fueled civil unrest across the United States. Drawing from the process-based model of policing, social cognitive theory, and past research on media effects, we assess the influence of viewing cell phone videos of police-citizen encounters on perceptions of law enforcement. Using quasi-

experimental methods and video footage of an actual police-citizen encounter captured on cell phones, the effects of viewing these videos are assessed using a series of repeated measure ANOVAs. Results indicate that viewing cell phone videos of police-citizen encounters significantly impacts perceptions of law enforcement, though little evidence of differing effects based on point-of-view, number of video exposures, or ordering of video exposures was found. The process-based model of policing should consider further incorporating the contributions of technology to provide a more holistic account of the factors influencing perceptions of police.

97. Paterson, C., (2007). 'Street-level Surveillance': Human Agency and the Electronic Monitoring of Offenders, *Surveillance and Society*, 4, 4, 314-328.

Abstract:

Recent years have witnessed an increase in new 'technologies of control' that decrease reliance upon labour intensive forms of policing. The electronic monitoring of offenders represents just one section of the expanding industry in 'techno-corrections' that incorporates elements of the private security, military and telecommunications industries. The surveillance capacity generated by these industries has diverted attention away from the role of human agency in the implementation of surveillance services. This paper is concerned with the reliance of 'technologies of control' upon 'street-level surveillance' which involves a shift in focus away from the capacity of surveillance technologies and towards the actions of agents of control, offenders and the local community, in ensuring the successful operation of electronic monitoring services.

98. Paterson, C. (2017), Tagging re-booted! Imagining the potential of victim-oriented electronic monitoring, *Probation Journal*, 64, 3, 226-241 DOI: 10.1177/0264550517711278.

Abstract:

Electronic monitoring (EM) technologies or 'tagging', as the ankle bracelet is known, have been subject to much experimentation across the criminal justice landscape, yet there remains a good deal of conjecture concerning the purpose and subsequent effectiveness of these technologies. This article calls for renewed consideration of both the potential and pitfalls of radio frequency (RF) and global positioning by satellite (GPS) EM technologies and provides a victim-oriented perspective on future developments in EM. The author proposes further interrogation of the penal assumptions that underpin thinking about the use of EM as well as analysis of recent police experimentation with the technology. The article concludes with a call for a clear and strong probation voice in the renewed debates about EM that can guide and support ethical and effective policy and practice.

99. Paterson, C., & Clamp, K. (2014), Innovating Responses to Managing Risk: Exploring the Potential of a Victim-Focused Policing Strategy, *Policing: A Journal of Policy and Practice,* 8, 1, 51-58. DOI: 10.1093/police/pat028

Abstract:

This article explores the potential benefits of developing partnerships with victims in managing threats to their personal safety via smart police use of electronic monitoring technologies. The central premise for this position is that traditional surveillance responses that seek to manage offending behaviour have limited effectiveness and do not create a sense of security for victims. Using a pilot project

currently underway in Buenos Aires, we extrapolate the potential implications of a victim-focused strategy for the policing role and the effectiveness of responses to high-risk repeat offences. The pilot project seeks to enhance victims' sense of their own safety, reduce the risk of repeat violence and develop indirect benefits for police legitimacy. Utilized in this way, there is significant potential for electronic monitoring to facilitate smarter policing and demand reduction.

100. Powell, A., & Henry, N. (2018) Policing technology-facilitated sexual violence against adult victims: police and service sector perspectives, *Policing and Society*, 28, 3, 291-307, DOI: 10.1080/10439463.2016.1154964

Abstract

To date, the majority of attention to technology-facilitated sexual violence (TFSV) in both policy and practice has been on child sexual exploitation and abuse. Far less attention has been paid to digital sexualised violence against adult members of the population. The aim of this paper is to examine police responses to these serious and emerging harms, which we identify as including the following: (1) online sexual harassment; (2) gender and sexuality-based harassment; (3) cyberstalking; (4) image-based sexual exploitation (including revenge pornography'); and (5) the use of communications technologies to coerce a victim into an unwanted sexual act. While these are variously criminal offences, unlawful civil behaviours or not subject to criminal or civil sanctions or remedies, we claim in this paper that they exist on a continuum of violence and yet the real' harms of TFSV are frequently minimised in practice. Drawing on 30 stakeholder interviews with police, legal services and domestic and sexual violence service sector providers, we explore the issues, challenges and promises of law enforcement in this area. We argue that greater

attention must be paid to recognising the serious harms of digital abuse and harassment; the role of criminal law in responding to these behaviours; and the importance of investing in police resources to adequately tackle these growing behaviours in a constantly shifting and amorphous digital era.

101. Ray, R., Marsh, K., & Powelson, C. (2017), Can Cameras Stop the Killings? Racial Differences in Perceptions of the Effectiveness of Body-Worn Cameras in Police Encounters. *Sociological Forum*, 32: 1032-1050. https://doi.org/10.1111/socf.12359

Abstract

Recent killings of blacks by police have renewed a national discussion about crime, racism, unjust treatment, and implicit bias. Outfitting police officers with body-worn cameras (BWC) is heralded by federal and state lawmakers as one solution to providing more transparency during police encounters. Missing from this discussion is what everyday citizens think about the potential effectiveness of BWC. Using data on residents of Prince George's County, Maryland, this study explores racial differences in views about police treatment and the effectiveness of BWC. We find that nonwhites report more fear of and mistreatment by the police than whites. Regarding BWC, we find that respondents are either supporters or skeptics. On one hand, respondents either believe that BWC will illuminate the difficulties of policing—police supporters—or create more transparency to hold officers more accountable for their actions—citizen supporters. On the other hand, skeptics fall into one of two types—respondents who think that BWC may put police officers more at risks—privacy skeptics—or those who do not see BWC as structurally changing the power dynamics between citizens and police officers—structural skeptics. We conclude by

discussing how BWC may operate as a solution to improve interactions between citizens and the police but not necessarily alter power relations.

102. Ridgeway, G. (2018), Policing in the Era of Big Data, *Annual Review of Criminology*, 1, 401-419, https://doi.org/10.1146/annurev-criminol-062217-114209

Abstract

Fifty years ago, the 1967 President's Commission on Law Enforcement and Administration of Justice urged the rapid adoption of information technology to improve the effectiveness, efficiency, and fairness of the criminal justice system, including policing. They predicted that we could make great progress on the challenge of crime if only we could deliver the right information to the right police officer at the right time. In this twenty-first century era of Big Data, all the technologies described in the 1967 Commission report are widely available and accessible to police departments. This review characterizes what Big Data means for policing, discusses the technologies making Big Data possible, describes how police departments are putting Big Data to use, and assesses how close we are coming to realizing the vision offered in 1967. Although police may be rich in data, we still need to improve the extraction of information and knowledge from that data and put them to use to decrease crime and improve clearance rates.

103. Rogers, C., & Scally, E. J. (2018), Police use of technology: insights from the literature, *International Journal of Emergency Services*, 7, 2, 100-110. https://doi.org/10.1108/IJES-03-2017-0012

Abstract

Purpose: The purpose of this paper is to consider the existing literature surrounding the use of technology in today's society to inform future developments across emergency services. Reference to the Police Service in particular will have a resonance for many other public agencies who are utilising more and more technology.

Design/methodology/approach: Literature from a policing background will be reviewed to discover the positive impacts and benefits attached to its use, the potential obstacles to its implantation, and how lessons from one agency may be of benefit to others.

Findings: The findings suggest that there appears to be attention required in the application of technology by public agencies, namely, workforce culture, training and budgets, and legislation which need to be addressed if the use of technology by public agencies is to be successful.

Originality/value: This paper seeks to learn lessons for the implementation technology by a public agency, namely, the police, in an attempt to inform other public bodies. By doing so, it is believed the lessons learned will make the applicatio n of such technologies more effective.

104. Rosenfeld, A., (2019). Are drivers ready for traffic enforcement drones? *Accident Analysis & Prevention,* 122, 199-206, https://doi.org/10.1016/j.aap.2018.10.006.

Abstract

Traffic enforcement drones reduce high-risk driving behavior which often leads to traffic crashes. However, the introduction of drones may face a public acceptance challenge which may severely hinder their potential impact. In this paper, we report and discuss the results of a drivers' survey, administered both in the US and Israel, regarding the benefits, concerns and policy considerations for the deployment of traffic enforcement drones. The results show that drivers perceive traffic enforcement drones as significantly more efficient and deterring compared to current aerial traffic enforcement resources (i.e., police helicopters) and comparable in quality to speed cameras. Privacy and safety are the main concerns expressed with regards to such technology, yet these concerns have been shown to be significantly relieved if traffic enforcement drones are restricted to interurban spaces. Interestingly, only a few Israeli participants object to the introduction of traffic enforcement drones to the traffic police's arsenal compared to about half of American participants. These results combine to suggest several practical guidelines for decision-makers which can facilitate the deployment of this potentially life-saving technology in the field.

105. Sahin, N. M., & Cubukcu, S. (2021), In-Car Cameras and Police Accountability in Use of Force Incidents. *J Police Crim Psych*. https://doi.org/10.1007/s11896-021-09472-9

Abstract

New policing technologies have generated solutions to many policing issues. In particular, portable camera systems (in-car or body-worn) have been offered as a tool to address the issue of police excessive use of force. It has been argued that police camera systems increase transparency in law enforcement and deter both police officers and citizens from engaging in undesirable behaviors during encounters. However, the question of how effective these technologies are in increasing the accountability of police departments still remains unanswered. Some argue that the use of camera systems to record police behavior does not create a significant reduction in excessive use-of-force complaints or does not serve as an effective accountability tool as expected. From this perspective, this study explores the impact of in-car camera usage on police use-of-force investigations. This research examines the impact of in-car cameras on the total, dismissed, and sustained excessive use-of-force complaints against 891 police departments in the USA with more than 100 sworn officers. We employed Law Enforcement Management and Administrative Statistics (LEMAS) 2007 dataset to conduct this analysis. We utilized negative binomial regression analysis in STATA 15 to examine whether the adoption of vehicle camera systems by police agencies has an impact on dismissed and sustained complaints of inappropriate use-of-force. We found that the adoption of in-car cameras correlates with the number of dismissed cases; however, we did not find any significant relationship between in-car camera usage and sustained cases. Police departments using in-car camera systems are more

likely to dismiss citizen complaints, rather than sustaining them. We concluded that video footages generated by in-car camera systems are inadequate in producing evidence to back up the complainants' claims or in generating proof of excessive use of force for further investigation. Our findings suggest that police departments should not solely rely on in-car cameras if they want to enhance accountability and unearth police misconduct within their department.

106. 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

Abstract

Unmanned aerial systems (that is, UAS or drones) have been increasingly proposed and used by federal and state law enforcement agencies as an evolving technology for general surveillance, crime detection and criminal investigations. However, the use of UAS technology, in general, and within the particular context of domestic policing activities raises serious concerns about personal privacy and the greater intrusion of new forms of `big brother' surveillance in people's daily lives. On the basis of a national survey, the current study provides empirical evidence on public attitudes about UAS usage in various policing activities. Socio-demographic differences in the public support for drone usage in this context are also examined. Our general findings of context-specific variability in public support for UAS usage in policing operations are discussed in terms of their implications for developing public policy.

107. Samuel, G., & Prainsack, B. (2019) Forensic DNA phenotyping in Europe: views “on the ground” from those who have a professional stake in the technology, *New Genetics and Society*, 38, 2, 119-141, DOI: 10.1080/14636778.2018.1549984

Abstract

Forensic DNA phenotyping (FDP) is an emerging technology that seeks to make probabilistic inferences regarding a person's observable characteristics ("phenotype") from DNA. The aim is to aid criminal investigations by helping to identify unknown suspected perpetrators, or to help with non-criminal missing persons cases. Here we provide results from the analysis of 36 interviews with those who have a professional stake in FDP, including forensic scientists, police officers, lawyers, government agencies and social scientists. Located in eight EU countries, these individuals were asked for their views on the benefits and problems associated with the prospective use of FDP. While all interviewees distinguished between those phenotypic tests perceived to either raise ethical, social or political concerns from those tests viewed as less ethically and socially problematic, there was wide variation regarding the criteria they used to make this distinction. We discuss the implications of this in terms of responsible technology development.

108. 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

Abstract

Information sharing and collaborative policing have become hot topics within policing circles, especially in the wake of such horrific events as school shootings and multiple murder cases. In response to growing concerns over inadequate information sharing and integrated policing, police organisations are actively centralising their services through the implementation of shared technologies (such as computer aided dispatch systems and record management systems). Drawing on interviews and participation observation within two technologically similar Canadian police services, we uncover the material, social and organisational barriers to information sharing and integrated policing. We conclude by arguing that technological anomalies arising from materiality and organisational practices uncovers a critical functional disconnect between the design and patrol officer use of information technologies.

109. Sandhu, A., & Fussey, P. (2021) The 'uberization of policing'? How police negotiate and operationalise predictive policing technology, *Policing and Society*, 31, 1, 66-81, DOI: 10.1080/10439463.2020.1803315

Abstract

Predictive policing generally refers to police work that utilises strategies, algorithmic technologies, and big data to generate near-future predictions about the people and places deemed likely to be involved in or experience crime. Claimed benefits of predictive policing centre on the technology's ability to enable pre-emptive police work by automating police decisions. The goal is that officers will rely on computer software and smartphone applications to instruct them about where and who to police just as Uber drivers rely on similar technologies to instruct them about where to pick up passengers. Unfortunately, little is known about the experiences of the in-

field users of predictive technologies. This article helps fill this gap by addressing the under researched area of how police officers engage with predictive technologies. As such, data is presented that outlines the findings of a qualitative study with UK police organisations involved in designing and trialing predictive policing software. Research findings show that many police officers have a detailed awareness of the limitations of predictive technologies, specifically those brought about by errors and biases in input data. This awareness has led many officers to develop a sceptical attitude towards predictive technologies and, in a few cases, these officers have expressed a reluctance to use

predictive software's ability to neutralise the subjectivity of police work overlooks the ongoing struggles of the police officer to assert their agency and mediate the extent to which predictions will be trusted and utilised.

110. Sandhu, A., & Haggerty, K. D. (2017). Policing on camera. *Theoretical Criminology*, 21, 1, 78–95. https://doi.org/10.1177/1362480615622531

Abstract

On any shift a police officer might be filmed by some combination of public or private surveillance cameras, including the cameras of individual citizens, activists, journalists, businesses, and a range of police-controlled cameras. This loosely coordinated camera infrastructure is part of the broader transformation of policing from a historically low visibility to an increasingly high visibility' occupation. This article reports on the findings of a participant-observation study of how police officers understand and respond to this transformation. We identify three distinct orientations, and highlight the multifaceted and contradictory relationship between

police officers and cameras. The study raises questions about the extent to which camera technologies represent a straightforward way to police the police.

111. Sheehey, B. (2019), Algorithmic paranoia: the temporal governmentality of predictive policing. *Ethics Inf Technol* 21, 49–58. https://doi.org/10.1007/s10676-018-9489-x

Abstract

In light of the recent emergence of predictive techniques in law enforcement to forecast crimes before they occur, this paper examines the temporal operation of power exercised by predictive policing algorithms. I argue that predictive policing exercises power through a paranoid style that constitutes a form of temporal governmentality. Temporality is especially pertinent to understanding what is ethically at stake in predictive policing as it is continuous with a historical racialized practice of organizing, managing, controlling, and stealing time. After first clarifying the concept of temporal governmentality, I apply this lens to Chicago Police Department's Strategic Subject List. This predictive algorithm operates, I argue, through a paranoid logic that aims to preempt future possibilities of crime on the basis of a criminal past codified in historical crime data.

112. Skogan, W. G., & Hartnett, S. M. (2005) The Diffusion of Information Technology in Policing, *Police Practice and Research*, 6, 5, 401-417, DOI: 10.1080/15614260500432949

Abstract

This study examines the diffusion of innovation among municipal police departments in northeastern Illinois. The opportunity to adopt an innovation arose when the

Chicago Police Department (CPD) opened access to elements of its new centralized Data Warehouse to other criminal justice agencies. There is a long history of research on the diffusion of innovation, and a number of recent projects have applied this work to policing. Like innovation studies generally, this paper presents the shape of the diffusion curve that describes the pace of adoption, and it examines factors associated with adoption and the extent to which the innovation was actually used. Adoption and extent of utilization proved to be largely independent processes. Involvement in cosmopolitan networks, experience with using databases for law enforcement, and the human capital capacities of the organizations influenced the adoption decision, while organizational resources and experience in using the system drove the level of actual use. The rapid growth of system utilization was apparently due to three factors: the active role played by the 'evangelist' representing the host department; the fact that access to the system was free; and because it primarily empowered detectives-who enjoy a privileged position in policing-and did not challenge the traditional mission and organization of participating agencies.

113. Singh, M. (2017) Mobile technologies for police tasks: An Australian study, *Journal of Organizational Computing and Electronic Commerce*, 27, 1, 66-80, DOI: 10.1080/10919392.2016.1263114

Abstract

Mobile technologies are increasingly adopted by information intensive organizations such as public police corporations to support the tasks of its employees, for information management and innovation. However, because police organizations are government organizations, technology decisions are largely made by managers and politicians with budget being a key factor. Therefore, whether the technologies

adopted are suitable for police tasks, and if they enhance performance, is generally not assessed. The aim of this research is to establish if mobile technologies support police tasks, and if Tablet PCs especially are suitable for specialist police tasks of the Criminal Investigators and Sexual Offence and Child Abuse Units. Guided by an interpretive paradigm and the theory of task technology fit, this research explores the use of Tablet PCs by the two police units for improved performance. Because information is critical for police tasks, data collected via focus groups establishes the impact of these technologies on case investigations, information management, and the performance of these units with the use of Tablet PCs. The contribution this study makes to mobile information systems is that if technology dimensions are suitable for information based tasks, the outcome is virtualization of processes through which improved performance is achieved due to reduced costs, transparency, teamwork, and quick and informed decisions. The findings of this research can be used by police organizations, as well as by other organizations, for effective implementation of mobile technologies.

114. Smykla, J. O., Crow, M. S., Crichlow, V. J. et al. (2016), Police Body-Worn Cameras: Perceptions of Law Enforcement Leadership. *Am J Crim Just,* 41, 424–443 https://doi.org/10.1007/s12103-015-9316-4

Abstract

Many people are enthusiastic about the potential benefits of police body-worn cameras (BWC). Despite this enthusiasm, however, there has been no research on law enforcement command staff perceptions of BWCs. Given the importance that law enforcement leadership plays in the decision to adopt and implement BWCs, it is necessary to assess their perceptions. This is the first study to measure law

enforcement leadership attitudes toward BWCs. The study relies on data collected from surveys administered to command staff representing local, state and federal law enforcement agencies in a large southern county. Among the major perceptual findings are that command staff believe BWCs will impact police officers' decisions to use force in encounters with citizens and police will be more reluctant to use necessary force in encounters with the public. Respondents also believe that use of BWCs is supported by the public because society does not trust police, media will use BWC data to embarrass police, and pressure to implement BWCs comes from the media. Perceptions of the impact of BWCs on safety, privacy, and police effectiveness are also discussed.

115. Saulnier, A, Lahay, R, McCarty, W. P., & Sanders, C. (2020), The RIDE study: Effects of body-worn cameras on public perceptions of police interactions. *Criminol Public Policy*, 19: 833– 854. https://doi.org/10.1111/1745-9133.12511

Abstract

Research Summary: During a brief interaction with motorists (i.e., a sobriety check), this study manipulated officer use (and declaration) of a body-worn camera (BWC) (present; absent) while documenting participant BWC recollection (correct; incorrect) to assess effects on motorists' perceptions of the encounter and of police more generally. Results (N = 361) demonstrate that perceptions of procedural justice were more favourable in the BWC-present condition when the entire sample was included in the analyses, but that this effect was not significant when focusing on the subset of the sample that correctly recollected BWC use (though the pattern of the effect was the same in both analyses). Policy Implications: In combination with results from

a handful of similar studies, this study's results suggest that BWCs may be a tool that can be leveraged to enhance public perceptions of encounters with police; however, more research is needed to substantiate this claim. In particular, the development of evidence-based policy on this matter necessitates continued studies that address issues such as sample imbalances (e.g., gender and minority status), length of the interaction studied (i.e., experimental dosage), and controlling for officer behavior.

116. 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

Abstract

Biometric facial recognition is an artificial intelligence technology involving the automated comparison of facial features, used by law enforcement to identify unknown suspects from photographs and closed circuit television. Its capability is expanding rapidly in association with artificial intelligence and has great potential to solve crime. However, it also carries significant privacy and other ethical implications that require law and regulation. This article examines the rise of biometric facial recognition, current applications and legal developments, and conducts an ethical analysis of the issues that arise. Ethical principles are applied to mediate the potential conflicts in relation to this information technology that arise between security, on the one hand, and individual privacy and autonomy, and democratic accountability, on the other. These can be used to support appropriate law and regulation for the technology as it continues to develop.

117. Stalcup, M., & Hahn, C. (2016). Cops, cameras, and the policing of ethics. *Theoretical Criminology*, 20, 4, 482–501. https://doi.org/10.1177/1362480616659814

Abstract

In this article, we explore how cameras are used in policing in the United States. We outline the trajectory of key new media technologies, arguing that cameras and social media together generate the ambient surveillance through which graphic violence is now routinely captured and circulated. Drawing on the work of Michel Foucault, we identify and examine intersections between video footage and police subjectivity in case studies of recruit training at the Washington state Basic Law Enforcement Academy and the Seattle Police Department's body-worn camera project. We analyze these cases in relation to the major arguments for and against initiatives to increase police use of cameras, outlining what we see as techno-optimistic and techno-pessimistic positions. Drawing on the pragmatism of John Dewey, we argue for a third position that calls for field-based inquiry into the specific co-production of socio-techno subjectivities.

118. Stone, K. E. (2018), Smart Policing and the Use of Body Camera Technology: Unpacking South Africa's Tenuous Commitment to Transparency, Policing: A Journal of Policy and Practice, 12, 1, 109-115, DOI: 10.1093/police/pax066.

Abstract:

In 2014, the Western Cape Department of Community Safety in South Africa launched the first pilot of the Smart Policing Project, which sought to reduce incidents of violence between private citizens and law enforcement officials by

attaching body-worn cameras (BWCs) to a small group of traffic officers throughout the province. In light of rising allegations of police brutality and deep-seated tensions between citizens and law enforcement officials, the Smart Policing Project received widespread support across the country. However, despite the appearance of a strengthening in police oversight, the ability of BWCs to hold police officers to account for acts of misconduct or criminality depends largely upon the existence of institutional policies governing usage, and a robust legislative framework for accessing information held by the state. Accordingly, the purpose of this article is to unpack South Africa's tenuous commitment to transparency by juxtaposing the reactions of law enforcement officials to wearing BWCs owned and operated by the state, versus being recorded by cell phones owned and operated by private citizens. The article begins by examining the context of police oversight in South Africa in an effort to demonstrate the rationale for introducing BWCs 20 years post-Apartheid. It then moves on to highlight inconsistencies in South Africa's right of access to information regime by exploring differences in the levels of protection afforded to records held by public bodies versus those held by private bodies under the country's access to information legislation. The article concludes by discussing the impact of those protections on the utility of BWCs in South Africa, and making recommendations on how to increase the effectiveness of BWCs in strengthening openness and transparency in policing.

119. Tanner, S., & Meyer, M. (2015). Police work and new 'security devices': A tale from the beat. *Security Dialogue*, 46, 4, 384–400. https://doi.org/10.1177/0967010615584256

Abstract

Mobile technologies have brought about major changes in police equipment and police work. If a utopian narrative remains strongly linked to the adoption of new technologies, often formulated as 'magic bullets' to real occupational problems, there are important tensions between their 'imagined' outcomes and the (unexpected) effects that accompany their daily 'practical' use by police officers. This article offers an analysis of police officers' perceptions and interactions with security devices. In so doing, it develops a conceptual typology of strategies for coping with new technology inspired by Le Bourhis and Lascoumes: challenging, neutralizing and diverting. To that purpose, we adopt an ethnographic approach that focuses on the discourses, practices and actions of police officers in relation to three security devices: the mobile digital terminal, the mobile phone and the body camera. Based on a case study of a North American municipal police department, the article addresses how these technological devices are perceived and experienced by police officers on the beat.

120. 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

Abstract

Purpose: The diffusion of innovations paradigm suggests that stakeholders' acceptance of a police innovation shapes how it spreads and impacts the larger criminal justice system. A lack of support by external stakeholders for police body-worn cameras (BWCs) can short-circuit their intended benefits. The purpose of this paper is to examine the perceptions of BWCs among non-police stakeholders who are impacted by the technology as well as how BWCs influence their daily work processes.

Design/methodology/approach: The authors conducted interviews and focus groups (n=41) in two US cities where the police department implemented BWCs. The interviewees range from courtroom actors (e.g. judges, prosecutors) to those who work with police in the field (e.g. fire and mental health), city leaders, civilian oversight members, and victim advocates.

Findings: External stakeholders are highly supportive of the new technology. Within the diffusion of innovations framework, this support suggests that the adoption of BWCs will continue. However, the authors also found the decision to implement BWCs carries unique consequences for external stakeholders, implying that a comprehensive planning process that takes into account the views of all stakeholders is critical.

Originality/value: Despite the recent diffusion of BWCs in policing, this is the first study to examine the perceptions of external stakeholders. More broadly, few criminologists have applied the diffusion of innovations framework to understand how technologies and other changes emerge and take hold in the criminal justice system. This study sheds light on the spread of BWCs within this framework and offers insights on their continued impact and consequences.

121. Todd, C., Bryce, J., & Franqueira, V. N. L. (2021) Technology, cyberstalking and domestic homicide: informing prevention and response strategies, *Policing and Society,* 31, 1, 82-99, DOI: 10.1080/10439463.2020.1758698

Abstract

An emerging concern in relation to the importance of technology and social media in everyday life relates to their ability to facilitate online and offline stalking, domestic violence and escalation to homicide. However, there has been little empirical research or policing and policy attention to this domain. This study examined the extent to which there was evidence of the role of technology and cyberstalking in domestic homicide cases based on the analysis of 41 Domestic Homicide Review (DHR) documents, made available by the Home Office (UK). Three interviews were also conducted with victims or family members of domestic homicide in the UK. It aimed to develop a deeper understanding of the role of technology in facilitating these forms of victimisation to inform further development of investigative practice, risk assessment and safeguarding procedures. Key themes identified by the thematic analysis undertaken related to behavioural and psychological indicators of cyberstalking, evidence of the role of technology in escalation to homicide and the digital capabilities of law enforcement. Overall, the results indicated that: (1) there was evidence of technology and social media playing a facilitating role in these behaviours, (2) the digital footprints of victims and perpetrators were often overlooked in police investigations and the DHR process and (3) determining the involvement of technology in such cases is important for risk assessment and earlier intervention to prevent escalation of behaviour to domestic homicide. It also indicates

the importance of further developing evidence-based approaches to preventing and responding for victims, the police and other practitioners.

122. Tulumello, S., & Iapaolo, F., (2021), Policing the future, disrupting urban policy today. Predictive policing, smart city, and urban policy in Memphis, *Urban Geography,* DOI: 10.1080/02723638.2021.1887634

Abstract:

Significant resources and efforts have been devoted, especially in the USA, to develop predictive policing programs. Predictive policing is, at the same time, one of the drivers of the birth, and the ultimate material enactment of, the anticipatory logics that are central to the smart city discourse. Quite surprisingly, however, critical analyses of the smart city have remained divorced from critical criminology and police studies. To fill this gap, this article sets out the first critical, in-depth empirical discussion of Blue CRUSH, a predictive policing program developed in Memphis (TN, USA), where its implementation intersects long-term austerity for urban policy. The article, first, shows that there is no evidence of Blue CRUSH's capacity to prevent crime, thus adding empirical material to skepticism over the role of predictive policing as a policy solution in the first place. And, second, it argues that, rather than making crime a matter of technological solutions, predictive policing shifts the politics therein - in short, it contributes to the expansion of policing into the field of urban policy at the same time as it disrupts present police work. These takeaways allow to further the critique of the salvific promises implicit in the smart city discourse.

123. 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

Abstract

In this paper, we discuss the present and future uses of intelligent facial surveillance (IFS) in law enforcement. We present an empirical and legally focused case study of live automated facial recognition technologies (LFR) in British policing. In Part I, we analyse insights from 26 frontline police officers exploring their concerns and current scepticism about LFR. We analyse recent UK case law on LFR use by police which raises concerns around human rights, data protection and anti-discrimination laws. In Part II, we consider frontline officers' optimism around future uses of LFR and explore emerging forms of IFS, namely emotional AI (EAI) technologies. A key novelty of the paper is our analysis on how the proposed EU AI Regulation (AIR) will shape future uses of IFS in policing. AIR makes LFR a prohibited form of AI and EAI use by law enforcement will be regulated as high-risk AI that has to comply with new rules and design requirements. Part III presents a series of 10 practical lessons, drawn from our reflections on the legal and empirical perspectives. These aim to inform any future law enforcement use of IFS in the UK and beyond.

124. Urquhart, L., Miranda, D., & Podoletz, L. (2022). Policing the smart home: The internet of things as 'invisible witnesses'. *Information Polity*. https://doi.org/10.3233/IP-211541

Abstract

In this paper, we develop the concept of smart home devices as 'invisible witnesses' in everyday life. We explore contemporary examples that highlight how smart

devices have been used by the police and unpack the socio-technical implications of using these devices in criminal investigations. We draw on several sociological, computing and forensics concepts to develop our argument. We consider the challenges of obtaining and interpreting trace evidence from smart devices; unpack the ways in which these devices are designed to be ‘invisible in use’; and consider the processes by which they become domesticated into everyday life. We also analyse the differentiated levels of control occupants have over home devices, and the surveillance impacts of making everyday life visible to third parties, particularly the police.

125. 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

Abstract

Despite the growing research interest in coproduction, some important gaps in our knowledge remain. Current literature is mainly concerned with either the citizens or professionals being involved in co-production, leaving unanswered the question how co-producers and professionals perceive each other’s engagement, and how this is reflected in their collaboration. This study aims to answer that question, conducting an exploratory case study on neighborhood watch schemes in a Dutch municipality. Empirical data are collected through group/individual interviews, participant observations, and document analysis. The results show that the perceptions citizens and professionals hold on their co-production partner’s engagement indeed impact

on the collaboration. Moreover, for actual collaboration to occur, citizens and professionals not only need to be engaged but also to make this engagement visible to their co-production partner. The article concludes with a discussion of the practical implications of these findings.

126. van ‘t Wout, E., Pieringer, C., Irribarra, D. T., Asahi, K., & Larroulet, P. (2021) Machine learning for policing: a case study on arrests in Chile, *Policing and Society,* 31, 9, 1036-1050, DOI: 10.1080/10439463.2020.1779270

Abstract

Police agencies expend considerable effort to anticipate future incidences of criminal behaviour. Since a large proportion of crimes are committed by a small group of individuals, preventive measures are often targeted on prolific offenders. There is a long-standing expectation that new technologies can improve the accurate identification of crime patterns. Here, we explore big data technology and design a machine learning algorithm for forecasting repeated arrests. The forecasts are based on administrative data provided by the national Chilean police agencies, including a history of arrests in Santiago de Chile and personal metadata such as gender and age. Excellent algorithmic performance was achieved with various supervised machine learning techniques. Still, there are many challenges regarding the design of the mathematical model, and its eventual incorporation into predictive policing will depend upon better insights into the effectiveness and ethics of preemptive strategies.

127. Wall, T. (2016) Ordinary Emergency: Drones, Police, and Geographies of Legal Terror. *Antipode*, 48, 1122– 1139. doi: 10.1111/anti.12228.

Abstract

This paper brings into conversation two ostensibly disparate geographies of state violence: the routine police surveillance and killing of members of the dangerous classes in the United States, an issue that is in no way new but nevertheless has gained increased attention over the last year with the Black Lives Matter movement; and the targeted drone strikes against terrorist suspects in the war on terror. By laying side by side the war drone and domestic police power, it becomes readily apparent that despite ostensible differencesforeign vs. domestic, war vs. peace, exceptional vs. normal, military vs. police, legal vs. extralegalthe unmanning of state violence gains much of its political and legal force from the language and categories that have long animated the routine policing of domestic territory. The paper calls for taking the violence of police power more seriously than many drone commentators have.

128. 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

Abstract

Studies of social media's impact on policing have emerged in several disciplines, including criminology, sociology, and communications. Despite their insight, there is no unified body of knowledge regarding this relationship. In an attempt to synthesize extant work, bring coherence to the field, and orient future scholarship, this article summarizes research on social media's implications for practices and perceptions of order maintenance. It does so by identifying how social media's technical affordances empower and constrain police services. By offering new opportunities

for surveillance, risk communication, and impression management, emergent technologies augment the police's control of their public visibility and that of the social world. However, they also provide unprecedented capacities to monitor the police and expose, circulate, and mobilize around perceived injustice, whether brutality, racial profiling, or other forms of indiscretion. Considering these issues promises to enhance knowledge on contemporary directions in social control, organizational communication, inequality, and collective action. Suggestions for future research are also explored.

129. Weaver, C. M., Chu, J. P., Lugo, A., Uyeda, N., Cha, Y. M., Zadonowics, T., & Giordano, B. (2021). Community-Based Participatory Research With Police: Development of a Tech-Enhanced Structured Suicide Risk Assessment and Communication Smartphone Application, *Law and Human Behavior*, 45, 5, 456-467. DOI: 10.1037/lhb0000470

Abstract:

Objective: Police officers initiate psychiatric holds following determination of suicide risk. Such referrals constitute direct decriminalization of mental illness at the single most efficient criminal justice system diversion point. However, system-level problems with this process highlight a need to further understand and improve this service connection juncture. The goal of the present study was to inform the development of a smartphone application designed to enhance police referrals of individuals experiencing suicide crises into treatment via culturally responsive structured professional judgment. Hypotheses: Given the developmental and qualitative nature of this study, there were no formal hypotheses tested. Research questions included the following: Would police officers broadly endorse concerns

about the care referral process? Would officers support the use of technology to assist with those concerns? And would officers raise concerns about the demands on time and expertise that would be placed on them to conduct thorough risk assessments? Method: Researchers used community-based participatory research (CBPR) methods to obtain police stakeholder-driven data through four focus groups with 47 police officers (76.6% male, 59.6% White, with a mean of 10.7 years of police employment) sampled from patrol and hostage negotiation units. Participants shared information about specific problems arising in the process through which police refer people to medical care, and they gave feedback on the beta version of a culturally responsive mobile app designed to streamline officers' evidence-based and culturally informed determinations of suicide risk. Results: Results, qualitatively coded using grounded theory methodology, yielded key considerations for police use of culturally responsive apps to divert individuals in suicidal crisis into treatment, including the need to maintain a balance between risk assessment and communication, allow for variance in time constraints, allow for flexibility in response and report options, account for inaccurate reports of suicide risk factors, maximize utility of the app's risk report output, incorporate sensitivity around cultural questions, and consider officers' safety in their use of the app in the field. Conclusions: The results illustrate a theoretically based (CBPR) approach to cross-disciplinary technology development to facilitate evidence-based assessments by law enforcement.

Public Significance Statement This study informs leveraging of digital technology and culturally responsive assessments to enhance police referrals of individuals experiencing suicide crises into treatment rather than incarceration. It specifically informs the development of a smartphone app designed to improve that process.

130. Vilendrer, S., Armano, A., Johnson, C. G. B., Favet, M., Safaeimli, N., Villasenor, J., Shaw, J. G., Hertelendy, A. J., Asch, S. M., & Mahoney, M. (2021), An App-Based Intervention to Support First Responders and Essential Workers During the COVID-19 Pandemic: Needs Assessment and Mixed Methods Implementation , *Journal of Medical Internet Research*, 23, 5, e26573 DOI: 10.2196/26573.

Abstract:

Background: The COVID-19 pandemic has created unprecedented challenges for first responders (eg, police, fire, and emergency medical services) and nonmedical essential workers (eg, workers in food, transportation, and other industries). Health systems may be uniquely suited to support these workers given their medical expertise, and mobile apps can reach local communities despite social distancing requirements. Formal evaluation of real-world mobile app-based interventions is lacking.

Objective: We aimed to evaluate the adoption, acceptability, and appropriateness of an academic medical center-sponsored app-based intervention (COVID-19 Guide App) designed to support access of first responders and essential workers to COVID-19 information and testing services. We also sought to better understand the COVID-19-related needs of these workers early in the pandemic.

Methods: To understand overall community adoption, views and download data of the COVID-19 Guide App were described. To understand the adoption, appropriateness, and acceptability of the app and the unmet needs of workers, semistructured qualitative interviews were conducted by telephone, by video, and in person with first responders and essential workers in the San Francisco Bay Area

who were recruited through purposive, convenience, and snowball sampling. Interview transcripts and field notes were qualitatively analyzed and presented using an implementation outcomes framework.

Results: From its launch in April 2020 to September 2020, the app received 8262 views from unique devices and 6640 downloads (80.4% conversion rate, 0.61% adoption rate across the Bay Area). App acceptability was mixed among the 17 first responders interviewed and high among the 10 essential workers interviewed. Select themes included the need for personalized and accurate information, access to testing, and securing personal safety. First responders faced additional challenges related to interprofessional coordination and a "culture of heroism" that could both protect against and exacerbate health vulnerability.

Conclusions: First responders and essential workers both reported challenges related to obtaining accurate information, testing services, and other resources. A mobile app intervention has the potential to combat these challenges through the provision of disease-specific information and access to testing services but may be most effective if delivered as part of a larger ecosystem of support. Differentiated interventions that acknowledge and address the divergent needs between first responders and non-first responder essential workers may optimize acceptance and adoption.

131. Whitehead, S., & Farrell, G., (2008), Anticipating Mobile Phone 'Smart Wallet' Crime: Policing and Corporate Social Responsibility, *Policing: A Journal of Policy and Practice*, 2, 2, 210–217, https://doi.org/10.1093/police/pan024

Abstract

Policing continues to struggle with the wave of mobile phone theft that emerged from the mid-1990s onwards. In this decade, the rate of increase may be waning, but the next wave may be approaching. Mobile phone smart wallets combine smart card technology with mobile phones, and the potential for identity theft and financial crime—and hence the attractiveness of theft—is likely to increase with smart wallets. This could spur new forms of theft, violence and other crimes. However, the market testing of technologies in Japan may be inappropriate for crime-proofing purposes, because of Japan's low crime rate. The criminogenic potential of smart card and mobile smart wallet technologies warrants further examination. If policing is to avoid a potential crime problem, discussions with manufacturers should begin before the problem takes hold.

132. White, M. D., Todak, N., & Gaub, J. E. (2018), Examining Body-Worn Camera Integration and Acceptance Among Police Officers, Citizens, and External Stakeholders. *Criminology & Public Policy*, 17, 649-677. https://doi.org/10.1111/1745-9133.12376

Abstract

We explore integration and acceptance of body-worn cameras (BWCs) among police, citizens, and stakeholders in one jurisdiction (Tempe, AZ) that adhered to the U.S. Department of Justice's (U.S. DOJ's) BWC Implementation Guide. We assess integration and acceptance through (a) officer surveys pre- and postdeployment, (b) interviews with citizens who had recent police encounters, and (c) interviews with external stakeholders. We also analyze (d) officer self-initiated contacts, (e) misdemeanor court case time to disposition, and (f) case outcomes. We found high levels of BWC acceptance across all groups. Officer proactivity remained consistent.

Time-to-case disposition and the rate of guilty outcomes both trended in positive directions.

Policy Implications: Although the results of early research on BWCs showed positive impacts, the findings from recent studies have been mixed. Implementation difficulties may explain the mixed results. Planning, implementation, and management of a BWC program are complex undertakings requiring significant resources. The technology also generates controversy, so the risk of implementation failure is substantial. The findings from our study demonstrate that adherence to the U.S. DOJ BWC Implementation Guide can lead to high levels of integration and acceptance among key stakeholders.

133. Wienroth, M., (2018) Governing anticipatory technology practices. Forensic DNA phenotyping and the forensic genetics community in Europe, *New Genetics and Society,* 37:2, 137-152, DOI: 10.1080/14636778.2018.1469975

Abstract

Forensic geneticists have attempted to make the case for continued investment in forensic genetics research, despite its seemingly consolidated evidentiary role in criminal justice, by shifting the focus to technologies that can provide intelligence. Forensic DNA phenotyping (FDP) is one such emerging set of techniques, promising to infer external appearance and ancestry of an unknown person. On this example, I consider the repertoire of anticipatory practices deployed by scientists, expanding the concept to not only focus on promissory but also include epistemic and operational aspects of anticipatory work in science. I explore these practices further as part of anticipatory self governance

efforts, attending to the European forensic genetics community and its construction of FDP as a reliable and legitimate technology field for use in delivering public goods around security and justice. In this context, I consider three types of ordering devices that translate anticipatory practices
into anticipatory self-governance.

134. Wienroth, M., (2020), Value beyond scientific validity: let's RULE (Reliability, Utility, LEgitimacy), Journal of Responsible Innovation, DOI: 10.1080/23299460.2020.1835152

Abstract

My perspective piece contributes to social studies of biometric technologies, and to studies on values and valuation within debates of responsible innovation. I reflect on innovation as
social practice where values are temporary settlements of considerations around validity, operability, and social compatibility of socio-technical innovations. As such, I propose a
practice-based approach to testing values in new technologies and their respective emerging practice and governance arrangements around Reliability, Utility and LEgitimacy (RULE).

These three values combine scientific with operational and social aspects of innovation as centre-points around which deliberative engagement can be facilitated between different societal perspectives, offering the opportunity to develop greater awareness of diverse and at times competing understandings of value. On the case study of forensic genetics – the use of genetic material and data for policing

purposes in security and justice contexts – I make the case for multi-perspectival, cross disciplinary, community-grounded deliberation based on RULE.

135. Williams, A., & Paterson, C. (2021). Social Development and Police Reform: Some Reflections on the Concept and Purpose of Policing and the Implications for Reform in the UK and USA, *Policing: A Journal of Policy and Practice*, 15, 2, 1565–1573, https://doi.org/10.1093/police/paaa087

Abstract

The increase in calls for police reform following the death of George Floyd has led to renewed debate about social inequality and the role of policing in society. Modern bureaucratic police systems emerged from locally administered structures and Anglo-American policing models continue to be aligned, to varying degrees, with the political, socio-cultural, legal, and ideological aspects of contemporary liberal democratic society with its emphasis on democratic localism and decentralised accountability. However, at a time when society is reimagining itself and technology, government, and nations are radically re-shaping themselves, a critical question is whether there is a sufficiently common philosophical and conceptual understanding of policing to support its development rather than just a common understanding of police functions. This is profoundly important when considering the current calls for reform of policing in the USA and other western democratic states. The article argues that there is an urgent need to reconsider how we conceptualize policing and its relationship with social development.

136. 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

Abstract

It is increasingly evident that if researchers and policymakers want to meaningfully develop an understanding of responsible innovation, we must first ask whether some sociotechnical systems should be developed, at all. Here I argue that systems like facial recognition, predictive policing, and biometrics are predicated on myriad human prejudicial biases and assumptions which must be named and interrogated prior to any innovation. Further, the notions of individual responsibility inherent in discussions of technological ethics and fairness overburden marginalized peoples with a demand to prove the reality of their marginalization. Instead, we should focus on equity and justice, valuing the experiential knowledge of marginalized peoples and optimally positioning them to enact deep, lasting change. My position aligns with those in Science, Technology, and Society (STS) which center diverse and situated knowledges, and is articulated together with calls for considering within science and engineering wider sociocultural concerns like justice and equality.

137. 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

Abstract

The digital revolution has transformed the potential reach and impact of criminal behaviour. Not only has it changed how people commit crimes but it has also created opportunities for new types of crimes to occur. Policymakers and criminal justice

institutions have struggled to keep pace with technological innovation and its impact on criminality. Criminal law and justice, as well as investigative and prosecution procedures, are often outdated and ill-suited to this type of criminality as a result. While technological solutions are being developed to detect and prevent digitally-enabled crimes, generic solutions are often unable to address the needs of criminal justice professionals and policymakers. Focussing specifically on social media, this article offers an exploratory investigation of the strengths and weaknesses of the current approach used to police offensive communications online. Drawing on twenty in-depth interviews with key criminal justice professionals in the United Kingdom, the authors discuss the substantial international challenges facing those seeking to police offensive social media content. They argue for greater cooperation between policymakers, social science and technology researchers to develop workable, innovative solutions to these challenges, and greater use of evidence to inform policy and practice.

138. 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

Abstract

We propose that late modern policing practices, that rely on neighbourhood intelligence, the monitoring of tensions, surveillance and policing by accommodation, need to be augmented in light of emerging cyber-neighbourhoods', namely social media networks. The 2011 riots in England were the first to evidence the widespread use of social media platforms to organise and respond to disorder. The police were

ill-equipped to make use of the intelligence emerging from these non-terrestrial networks and were found to be at a disadvantage to the more tech-savvy rioters and the general public. In this paper, we outline the development of the tension engine' component of the Cardiff Online Social Media ObServatroy (COSMOS). This engine affords users with the ability to monitor social media data streams for signs of high tension which can be analysed in order to identify deviations from the norm' (levels of cohesion/low tension). This analysis can be overlaid onto a palimpsest of curated data, such as official statistics about neighbourhood crime, deprivation and demography, to provide a multidimensional picture of the terrestrial' and cyber' streets. As a consequence, this neighbourhood informatics' enables a means of questioning official constructions of civil unrest through reference to the user-generated accounts of social media and their relationship to other, curated, social and economic data.

139. Wilson-Kovacs, D. (2021), Digital media investigators: challenges and opportunities in the use of digital forensics in police investigations in England and Wales, *Policing: An International Journal*, 44, 4, 669-682. https://doi.org/10.1108/PIJPSM-02-2021-0019

Abstract

Purpose - In-depth knowledge about specific national approaches to using digital evidence in investigations is scarce. A clearer insight into the organisational barriers and professional challenges experienced, alongside a more detailed picture of how digital evidence can help police investigations are required to empirically substantiate claims about how digital technologies are changing the face of criminal investigations. The paper aims to focus on the introduction of digital media

investigators to support investigating officers with the collection and interpretation of digital evidence.

Design/methodology/approach - Drawing on ethnographic and interview data collected as part of an Economic and Social Research Council-funded project on the application of digital forensics expertise in policing in England and Wales, this paper examines the changing face of investigations in relation to escalating digital demand.

Findings - The analysis presents the national and regional organisational parameters of deploying digital expertise in criminal investigation and examines some of the challenges of being a digital media investigator (DMI). Through testimonies from DMIs, digital forensic practitioners, investigating and senior officers and forensic managers, the analysis explores the organisational tensions in the collection, processing, interpretation and use of information from digital devices for evidential purposes.

Research limitations/implications -The paper offers an empirical basis for the comparative study of how the DMI role has been implemented by law enforcement agencies and its fit within broader institutional considerations and processes.

Practical implications - The development of the DMI role has raised questions about the supply of digital expertise, especially to volume crime investigations, and tensions around occupational divisions between scientific and operational units.

Social implications - The findings show that while the introduction of the DMI role was much needed, the development of this valuable provision within each force and the resources available require sustained and coordinated support to protect these professionals and retain their skills.

Originality/value - This study contributes to the growing sociological and criminological literature with an ethnographically based perspective into the

organisational and occupational tensions in the identification and processing of digital evidence in England and Wales.

140. Wolfe, M. (2021), Policing The Lost: The Emergence of Missing Persons and the Classification of Deviant Absence. *Theor Soc*. https://doi.org/10.1007/s11186-021-09466-w

Abstract

In the mid-19(th) century, increases in global migration and mobility produced a discernable rise in the number of ambiguous absences. This shift, combined with a novel expectation, linked to improved communications technology, that such absences might be resolved engendered the emergence of missing persons as a social category. A demand on the part of families of the missing that the state aid in their location would produce a Bourdieusian classification struggle over how to define and categorize this new mass of absences. At issue would be whether an ambiguously absent individual was merely absent, as a routine component of social life, or whether the individual merited legitimation by the state as a new form of deviant: a "missing" person. Scholars have described the emerging administrative state's enhanced powers of surveillance and classification and its persistent inclination to render their populations, in James Scott's phrase, "legible." Brought to the attention of the state, missing persons represented a body of people who had conspicuously fallen out of official sight. Yet, instead of attempting to fix this omission by gathering additional information on the lost - to, in effect, see the missing - as theories of the state would lead us to expect, the state chose to look away. In the United States, the state, in the form of municipal police departments, resisted classifying absences as cases of missingness and pushed back against families'

requests for aid. Leveraging the inherently ambiguous characteristics of the missing, the state promoted a definition of missing persons that conveniently freed it from the burden of managing an unmanageable population. In this article, drawing from archival data, I challenge prevailing theories of the modern state that emphasize its avidly classificatory nature by offering a case in which legibility was strategically withheld and a population was, in service of state interests, intentionally obscured. Only after the state lost its symbolic monopoly and the category was raced and gendered, becoming, in public discourse, associated with a socially valuable demographic - namely, young, white women - would the state, facing a threat to its legitimacy, deem the missing as worthy of being seen.

141. Woods, P., Leidl, D., Luimes, J., & Butler, L. (2019). Exploring the Delivery of Healthcare in the Police Detention Center Through Remote Presence Technology, *Journal of Forensic Nursing*, 15, 1, 26-34. doi: 10.1097/JFN.0000000000000217

Abstract

Introduction: There is overwhelming evidence to support the delivery of high-quality health service at a lower cost with the use of advanced technologies. Implementing remote presence technology to expand clinical care has been fraught with barriers that limit interprofessional collaboration and optimal client outcomes. In Canada, government ministries responsible for correctional services, policing, and health are well positioned to link federal, provincial, and regional services to enhance service delivery at the point of care for individuals detained within the justice system. Using remote presence technology to link the detention center with relevant health services such as the emergency room has the potential to open up a new care pathway.

Research Question: The key research question was how a new intervention pathway for individuals detained in police service detention centers could be implemented.
Research Design: Utilizing an exploratory qualitative research design, interviews were undertaken with 12 police service and six healthcare participants. Data were transcribed and thematically analyzed.
Findings: Four main themes emerged and included role conflict, risk management, resource management, and access to services. A number of collaborative learning partnerships were identified by the participants.

142. Wright, J. (2021). Suspect AI: Vibraimage, Emotion Recognition Technology and Algorithmic Opacity. *Science, Technology and Society*. https://doi.org/10.1177/09717218211003411

Abstract

Vibraimage is a digital system that quantifies a subject's mental and emotional state by analysing video footage of the movements of their head. Vibraimage is used by police, nuclear power station operators, airport security and psychiatrists in Russia, China, Japan and South Korea, and has been deployed at two Olympic Games, a FIFA World Cup and a G7 Summit. Yet there is no reliable empirical evidence for its efficacy; indeed, many claims made about its effects seem unprovable. What exactly does vibraimage measure and how has it acquired the power to penetrate the highest profile and most sensitive security infrastructure across Russia and Asia? I first trace the development of the emotion recognition industry, before examining attempts by vibraimage's developers and affiliates scientifically to legitimate the technology, concluding that the disciplining power and corporate value of vibraimage are generated through its very opacity, in contrast to increasing demands across the

social sciences for transparency. I propose the term ‘suspect artificial intelligence (AI)’ to describe the growing number of systems like vibraimage that algorithmically classify suspects/non-suspects, yet are themselves deeply suspect. Popularising this term may help resist such technologies’ reductivist approaches to ‘reading’—and exerting authority over—emotion, intentionality and agency.

143. Wright, J. E., & Headley, A. M. (2021). Can Technology Work for Policing? Citizen Perceptions of Police-Body Worn Cameras. *The American Review of Public Administration,* 51, 1, 17–27. https://doi.org/10.1177/0275074020945632

Abstract

Recent incidents between police and people of color have further strained police–community relationships. Scholars, practitioners, activists, policy makers, and several police departments have advocated for the implementation of body-worn cameras (BWC), a technological adoption promoted to address growing mistrust in the United States. This article examines perception of this technological adoption through 40 in-depth interviews in Washington, D.C. Furthermore, this article uses the context of police BWC to explore how the integration of technological advancements impacts the relationships between communities and local governments—namely police departments. The evidence suggests that residents believe BWC should improve officer behavior and increase police legitimacy, but cameras will not increase trust between police and the community. Based on the findings, this research identifies the limitations of BWC technology and assesses potential collaborative strategies available for police organizations related to the adoption and use of BWC.

144. Young, J. T. N., & Ready, J. T. (2015). Diffusion of Ideas and Technology: The Role of Networks in Influencing the Endorsement and Use of On-Officer Video Cameras. *Journal of Contemporary Criminal Justice*, 31, 3, 243–261. https://doi.org/10.1177/1043986214553380

Abstract

On-officer videos, or body cameras, can provide objective accounts of interactions among police officers and the public. Police leadership tends to view this emerging technology as an avenue for resolving citizen complaints and prosecuting offenses where victims and witnesses are reluctant to testify. However, getting endorsement from patrol officers is difficult. These incongruent cognitive frames are a cultural barrier to the utilization of innovative technologies. Understanding the mechanisms that lead to the deconstruction of these barriers is essential for the integration of technology into organizations. Using affiliation data collected from a large police department in Southwestern United States over a 4-month period, we find that interactions with other officers provide a conduit for facilitating cognitive frames that increase camera legitimacy.

Part C- Abstracts Selected for Inclusion from the Supplementary Literature Search Focusing on the Health and Children and Families' Sectors

*Health Sector*

1. Aicardi, C., Fothergill, T., Rainey, S., Carsten Stahl, B., and Harris, E., (2018), Accompanying technology development in the Human Brain Project: From foresight to ethics management, Futures 102, 114-124. https://doi.org/10.1016/j.futures.2018.01.005.

Abstract

This paper addresses the question of managing the existential risk potential of general Artificial Intelligence (AI), as well as the more near-term yet hazardous and disruptive implications of specialised AI, from the perspective of a particular research project that could make a significant contribution to the development of Artificial Intelligence (AI): the Human Brain Project (HBP), a ten-year Future and Emerging Technologies Flagship of the European Commission. The HBP aims to create a digital research infrastructure for brain science, cognitive neuroscience, and brain-inspired computing. This paper builds on work undertaken in the HBP's Ethics and Society subproject (SP12). Collaborators from two activities in SP12, Foresight and Researcher Awareness on the one hand, and Ethics Management on the other, use the case of machine intelligence to illustrate key aspects of the dynamic processes through which questions of ethics and society, including existential risks, are approached in the organisational context of the HBP. The overall aim of the paper is to provide practice-based evidence, enriched by self-reflexive assessment of the

approach used and its limitations, for guiding policy makers and communities who are, and will be, engaging with such questions.

2. 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

Abstract

Background: Smart-home technologies, comprising environmental sensors, wearables and video are attracting interest in home healthcare delivery. Development of such technology is usually justified on the basis of the technology's potential to increase the autonomy of people living with long-term conditions. Studies of the ethics of smart-homes raise concerns about privacy, consent, social isolation and equity of access. Few studies have investigated the ethical perspectives of smart-home engineers themselves. By exploring the views of engineering researchers in a large smart-home project, we sought to contribute to dialogue between ethics and the engineering community.

Methods: Either face-to-face or using Skype, we conducted in-depth qualitative interviews with 20 early- and mid-career smart-home researchers from a multi-centre smart-home project, who were asked to describe their own experience and to reflect more broadly about ethical considerations that relate to smart-home design. With participants' consent, interviews were audio-recorded, transcribed and analysed using a thematic approach.

Results: Two overarching themes emerged: in 'Privacy', researchers indicated that they paid close attention to negative consequences of potential unauthorised

information sharing in their current work. However, when discussing broader issues in smart-home design beyond the confines of their immediate project, researchers considered physical privacy to a lesser extent, even though physical privacy may manifest in emotive concerns about being watched or monitored. In ‘Choice’, researchers indicated they often saw provision of choice to end-users as a solution to ethical dilemmas. While researchers indicated that choices of end-users may need to be restricted for technological reasons, ethical standpoints that restrict choice were usually assumed and embedded in design.

Conclusions: The tractability of informational privacy may explain the greater attention that is paid to it. However, concerns about physical privacy may reduce acceptability of smart-home technologies to future end-users. While attention to choice suggests links with privacy, this may misidentify the sources of privacy and risk unjustly burdening end-users with problems that they cannot resolve. Separating considerations of choice and privacy may result in more satisfactory treatment of both. Finally, through our engagement with researchers as participants this study demonstrates the relevance of (bio)ethics as a critical partner to smart-home engineering.

3. Blease C, Kaptchuk T. J., Bernstein, M. H, Mandl, K. D., Halamka, J. D., Des Roches, C. M., (2019). Artificial Intelligence and the Future of Primary Care: Exploratory Qualitative Study of UK General Practitioners’ Views, J Med Internet Res, 21, (3):e12802, doi: 10.2196/12802

Abstract

Background: The potential for machine learning to disrupt the medical profession is the subject of ongoing debate within biomedical informatics and related fields.

Objective: This study aimed to explore general practitioners' (GPs') opinions about the potential impact of future technology on key tasks in primary care.

Methods: In June 2018, we conducted a Web-based survey of 720 UK GPs' opinions about the likelihood of future technology to fully replace GPs in performing 6 key primary care tasks, and, if respondents considered replacement for a particular task likely, to estimate how soon the technological capacity might emerge. This study involved qualitative descriptive analysis of written responses ("comments") to an open-ended question in the survey.

Results: Comments were classified into 3 major categories in relation to primary care: (1) limitations of future technology, (2) potential benefits of future technology, and (3) social and ethical concerns. Perceived limitations included the beliefs that communication and empathy are exclusively human competencies; many GPs also considered clinical reasoning and the ability to provide value-based care as necessitating physicians' judgments. Perceived benefits of technology included expectations about improved efficiencies, in particular with respect to the reduction of administrative burdens on physicians. Social and ethical concerns encompassed multiple, divergent themes including the need to train more doctors to overcome workforce shortfalls and misgivings about the acceptability of future technology to patients. However, some GPs believed that the failure to adopt technological innovations could incur harms to both patients and physicians.

Conclusions: This study presents timely information on physicians' views about the scope of artificial intelligence (AI) in primary care. Overwhelmingly, GPs considered the potential of AI to be limited. These views differ from the predictions of biomedical informaticians. More extensive, stand-alone qualitative work would provide a more in-depth understanding of GPs' views.

4. De Togni, G., Erikainen, S., Chan, S., and Cunningham-Burley, S. (2021), What makes AI 'intelligent' and 'caring'? Exploring affect and relationality across three sites of intelligence and care, *Social Science & Medicine*, 277, 113874, https://doi.org/10.1016/j.socscimed.2021.113874.

Abstract

This paper scrutinises how AI and robotic technologies are transforming the relationships between people and machines in new affective, embodied and relational ways. Through investigating what it means to exist as human 'in relation' to AI across health and care contexts, we aim to make three main contributions. (1) We start by highlighting the complexities of philosophical issues surrounding the concepts of "artificial intelligence" and "ethical machines." (2) We outline some potential challenges and opportunities that the creation of such technologies may bring in the health and care settings. We focus on AI applications that interface with health and care via examples where AI is explicitly designed as an 'augmenting' technology that can overcome human bodily and cognitive as well as socio-economic constraints. We focus on three dimensions of 'intelligence' - physical, interpretive, and emotional - using the examples of robotic surgery, digital pathology, and robot caregivers, respectively. Through investigating these areas, we interrogate the social context and implications of human-technology interaction in the interrelational sphere of care practice. (3) We argue, in conclusion, that there is a need for an interdisciplinary mode of theorising 'intelligence' as relational and affective in ways that can accommodate the fragmentation of both conceptual and material boundaries between human and AI, and human and machine. Our aim in investigating these sociological, philosophical and ethical questions is primarily to

explore the relationship between affect, relationality and ‘intelligence,’ the intersection and integration of ‘human’ and ‘artificial’ intelligence, through an examination of how AI is used across different dimensions of intelligence. This allows us to scrutinise how ‘intelligence’ is ultimately conveyed, understood and (technologically or algorithmically) configured in practice through emerging relationships that go beyond the conceptual divisions between humans and machines, and humans vis-à-vis artificial intelligence-based technologies.

5. 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

Abstract

While emerging digital health technologies offer researchers new avenues to collect real time data, little is known about current ethical dimensions, considerations, and challenges

that are associated with conducting digital data collection in research with minors. As such,

this paper reports the findings of a scoping review which explored existing literature to canvass current ethical issues that arise when using digital data collection in research with

minors. Scholarly literature was searched using electronic academic databases for articles

that provided explicit ethical analysis or presented empirical research that directly

addressed ethical issues related to digital data collection used in research with minors. After
screening 1,156 titles and abstracts, and reviewing 73 full-text articles, 20 articles were
included in this review. Themes which emerged across the reviewed literature included:
consent, data handling, minors' data rights, observing behaviors that may result in risk of
harm to participants or others, private versus public conceptualizations of data generated
through social media, and gatekeeping. Our findings indicate a degree of uncertainty which
invariably exists with regards to the ethics of research that involves minors and digital technology. The reviewed literature suggests that this uncertainty can often lead to the preclusion of minors from otherwise important lines of research inquiry. While uncertainty warrants ethical consideration, increased ethical scrutiny and restricting the conduct of such research raises its own ethical challenges. We conclude by discussing and recommending the ethical merits of co-producing ethical practice between researchers and minors as a mechanism to proceed with such research while addressing concerns around uncertainty.

6. Fukuda-Parr, S. and Gibbons, E. (2021), Emerging Consensus on 'Ethical AI': Human Rights Critique of Stakeholder Guidelines. Glob Policy, 12: 32-44. https://doi.org/10.1111/1758-5899.12965

Abstract

Voluntary guidelines on ‘ethical practices’ have been the response by stakeholders to address the growing concern over harmful social consequences of artificial intelligence and digital technologies. Issued by dozens of actors from industry, government and professional associations, the guidelines are creating a consensus on core standards and principles for ethical design, development and deployment of artificial intelligence (AI). Using human rights principles (equality, participation and accountability) and attention to the right to privacy, this paper reviews 15 guidelines preselected to be strongest on human rights, and on global health. We find about half of these ground their guidelines in international human rights law and incorporate the key principles; even these could go further, especially in suggesting ways to operationalize them. Those that adopt the ethics framework are particularly weak in laying out standards for accountability, often focusing on ‘transparency’, and remaining silent on enforceability and participation which would effectively protect the social good. These guidelines mention human rights as a rhetorical device to obscure the absence of enforceable standards and accountability measures, and give their attention to the single right to privacy. These ‘ethics’ guidelines, disproportionately from corporations and other interest groups, are also weak on addressing inequalities and discrimination. We argue that voluntary guidelines are creating a set of de facto norms and re-interpretation of the term ‘human rights’ for what would be considered ‘ethical’ practice in the field. This exposes an urgent need for action by governments and civil society to develop more rigorous standards and regulatory measures, grounded in international human rights frameworks, capable of holding Big Tech and other powerful actors to account.

7. Gooding, P., (2019), Mapping the rise of digital mental health technologies: Emerging issues for law and society, International Journal of Law and Psychiatry, 67, 101498, https://doi.org/10.1016/j.ijlp.2019.101498.

Abstract

The use of digital technologies in mental health initiatives is expanding, leading to calls for clearer legal and regulatory frameworks. However, gaps in knowledge about the scale and nature of change impede efforts to develop responsible public governance in the early stages of what may be the mass uptake of 'digital mental health technologies'. This article maps established and emerging technologies in the mental health context with an eye to locating major socio-legal issues. The paper discusses various types of technology, including those designed for information sharing, communication, clinical decision support, 'digital therapies', patient and/or population monitoring and control, bio-informatics and personalised medicine, and service user health informatics. The discussion is organised around domains of use based on the actors who use the technologies, and those on whom they are used. These actors go beyond mental health service users and practitioners/service providers, and include health and social system or resource managers, data management services, private companies that collect personal data (such as major technology corporations and data brokers), and multiple government agencies and private sector actors across diverse fields of criminal justice, education, and so on. The mapping exercise offers a starting point to better identify cross-cutting legal, ethical and social issues at the convergence of digital technology and contemporary mental health practice.

8. Kaplan, B. (2022). Ethics, Guidelines, Standards, and Policy: Telemedicine, COVID-19, and Broadening the Ethical Scope. Cambridge Quarterly of Healthcare Ethics, 31(1), 105-118. doi:10.1017/S0963180121000852

Abstract

The coronavirus crisis is causing considerable disruption and anguish. However, the COVID-19 pandemic and consequent explosion of telehealth services also provide an unparalleled opportunity to consider ethical, legal, and social issues (ELSI) beyond immediate needs. Ethicists, informaticians, and others can learn from experience, and evaluate information technology practices and evidence on which to base policy and standards, identify significant values and issues, and revise ethical guidelines. This paper builds on professional organizations' guidelines and ELSI scholarship to develop emerging concerns illuminated by current experience. Four ethical themes characterized previous literature: quality of care and the doctor–patient relationship, access, consent, and privacy. More attention is needed to these and to expanding the scope of ethical analysis to include health information technologies. An applied ethics approach to ELSI would addresses context-specific issues and the relationships between people and technologies, and facilitate effective and ethical institutionalization of telehealth and other health information technologies.

9. 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

Abstract

An array of technology-based interventions has increasingly become available to support family caregivers, primarily focusing on health and well-being, social isolation, financial, and psychological support. More recently the emergence of new technologies such as mobile and cloud, robotics, connected sensors, virtual/augmented/mixed reality, voice, and the evermore ubiquitous tools supported by advanced data analytics, coupled with the integration of multiple technologies through platform solutions, have opened a new era of technology-enabled interventions that can empower and support family caregivers. This paper proposes a conceptual framework for identifying and addressing the challenges that may need to be overcome to effectively apply technology-enabled solutions for family caregivers. The paper identifies a number of challenges that either moderate or mediate the full use of technologies for the benefit of caregivers. The challenges include issues related to equity, inclusion, and access; ethical concerns related to privacy and security; political and regulatory factors affecting interoperability and lack of standards; inclusive/human-centric design and issues; and inherent economic and distribution channel difficulties. The paper concludes with a summary of research questions and issues that form a framework for global research priorities.

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

Abstract

Discussion about vulnerable individuals and communities spread from research ethics to consumer law and human rights. According to many theoreticians and practitioners, the framework of vulnerability allows formulating an alternative language to articulate problems of inequality, power imbalances and social injustice.

Building on this conceptualisation, we try to understand the role and potentiality of the notion of vulnerable data subjects. The starting point for this reflection is wide-ranging development, deployment and use of data-driven technologies that may pose substantial risks to human rights, the rule of law and social justice. Implementation of such technologies can lead to discrimination systematic marginalisation of different communities and the exploitation of people in particularly sensitive life situations. Considering those problems, we recognise the special role of personal data protection and call for its vulnerability-aware interpretation. This article makes three contributions. First, we examine how the notion of vulnerability is conceptualised and used in the philosophy, human rights and European law. We then confront those findings with the presence and interpretation of vulnerability in data protection law and discourse. Second, we identify two problematic dichotomies that emerge from the theoretical and practical application of this concept in data protection. Those dichotomies reflect the tensions within the definition and manifestation of vulnerability. To overcome limitations that arose from those two dichotomies we support the idea of layered vulnerability, which seems compatible with the GDPR and the risk-based approach. Finally, we outline how the notion of vulnerability can influence the interpretation of particular provisions in the GDPR. In this process, we focus on issues of consent, Data Protection Impact Assessment, the role of Data Protection Authorities, and the participation of data subjects in the decision making about data processing.

11. 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

Abstract

Aim: To develop a consensus paper on the central points of an international invitational think-tank on nursing and artificial intelligence (AI).

Methods: We established the Nursing and Artificial Intelligence Leadership (NAIL) Collaborative, comprising interdisciplinary experts in AI development, biomedical ethics, AI in primary care, AI legal aspects, philosophy of AI in health, nursing practice, implementation science, leaders in health informatics practice and international health informatics groups, a representative of patients and the public, and the Chair of the ITU/WHO Focus Group on Artificial Intelligence for Health. The NAIL Collaborative convened at a 3-day invitational think tank in autumn 2019. Activities included a pre-event survey, expert presentations and working sessions to identify priority areas for action, opportunities and recommendations to address these. In this paper, we summarize the key discussion points and notes from the aforementioned activities.

Implications for nursing: Nursing's limited current engagement with discourses on AI and health posts a risk that the profession is not part of the conversations that have potentially significant impacts on nursing practice.

Conclusion: There are numerous gaps and a timely need for the nursing profession to be among the leaders and drivers of conversations around AI in health systems.

Impact: We outline crucial gaps where focused effort is required for nursing to take a leadership role in shaping AI use in health systems. Three priorities were identified that need to be addressed in the near future: (a) Nurses must understand the relationship between the data they collect and AI technologies they use; (b) Nurses need to be meaningfully involved in all stages of AI: from development to implementation; and (c) There is a substantial untapped and an unexplored potential for nursing to contribute to the development of AI technologies for global health and humanitarian efforts.

12. Saheb, T., Saheb, T., O. Carpenter, D., (2021), Mapping research strands of ethics of artificial intelligence in healthcare: A bibliometric and content analysis. Computers in Biology and Medicine, 135, 104660, https://doi.org/10.1016/j.compbiomed.2021.104660.

Abstract

The growth of artificial intelligence in promoting healthcare is rapidly progressing. Notwithstanding its promising nature, however, AI in healthcare embodies certain ethical challenges as well. This research aims to delineate the most influential elements of scientific research on AI ethics in healthcare by conducting bibliometric, social network analysis, and cluster-based content analysis of scientific articles. Not only did the bibliometric analysis identify the most influential authors, countries, institutions, sources, and documents, but it also recognized four ethical concerns associated with 12 medical issues. These ethical categories are composed of normative, meta-ethics, epistemological and medical practice. The content analysis complemented this list of ethical categories and distinguished seven more ethical categories: ethics of relationships, medico-legal concerns, ethics of robots, ethics of

ambient intelligence, patients' rights, physicians' rights, and ethics of predictive analytics. This analysis likewise identified 40 general research gaps in the literature and plausible future research strands. This analysis furthers conversations on the ethics of AI and associated emerging technologies such as nanotech and biotech in healthcare, hence, advances convergence research on the ethics of AI in healthcare. Practically, this research will provide a map for policymakers and AI engineers and scientists on what dimensions of AI-based medical interventions require stricter policies and guidelines and robust ethical design and development.

13. Samuel, G., & Prainsack, B. (2019) Forensic DNA phenotyping in Europe: views "on the ground" from those who have a professional stake in the technology, *New Genetics and Society*, 38:2, 119-141, DOI: 10.1080/14636778.2018.1549984

Abstract

Forensic DNA phenotyping (FDP) is an emerging technology that seeks to make probabilistic inferences regarding a person's observable characteristics ("phenotype") from DNA. The aim is to aid criminal investigations by helping to identify unknown suspected perpetrators, or to help with non-criminal missing persons cases. Here we provide results from the analysis of 36 interviews with those who have a professional stake in FDP, including forensic scientists, police officers, lawyers, government agencies and social scientists. Located in eight EU countries, these individuals were asked for their views on the benefits and problems associated with the prospective use of FDP. While all interviewees distinguished between those phenotypic tests perceived to either raise ethical, social or political concerns from those tests viewed as less ethically and socially problematic, there was wide

variation regarding the criteria they used to make this distinction. We discuss the implications of this in terms of responsible technology development.

14. 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

Abstract

Background: Electronic health records (EHRs) are increasingly implemented internationally, whereas digital sharing of EHRs with service users (SUs) is a relatively new practice. Studies of patient-accessible EHRs (PAEHRs)—often referred to as open notes—have revealed promising results within general medicine settings. However, studies carried out in mental health care (MHC) settings highlight several ethical and practical challenges that require further exploration.

Objective: This scoping review aims to map available evidence on PAEHRs in MHC. We seek to relate findings with research from other health contexts, to compare different stakeholders' perspectives, expectations, actual experiences with PAEHRs, and identify potential research gaps.

Methods: A systematic scoping review was performed using 6 electronic databases. Studies that focused on the digital sharing of clinical notes or EHRs with people affected by mental health conditions up to September 2021 were included. The Mixed Methods Appraisal Tool was used to assess the quality of the studies. The PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) Extension for Scoping Reviews guided narrative synthesis and reporting of findings.

Results: Of the 1034 papers screened, 31 were included in this review. The studies used mostly qualitative methods or surveys and were predominantly published after 2018 in the United States. PAEHRs were examined in outpatient (n=29) and inpatient settings (n=11), and a third of all research was conducted in Veterans Affairs Mental Health. Narrative synthesis allowed the integration of findings according to the different stakeholders. First, SUs reported mainly positive experiences with PAEHRs, such as increased trust in their clinician, health literacy, and empowerment. Negative experiences were related to inaccurate notes, disrespectful language use, or uncovering of undiscussed diagnoses. Second, for health care professionals, concerns outweigh the benefits of sharing EHRs, including an increased clinical burden owing to more documentation efforts and possible harm triggered by reading the notes. Third, care partners gained a better understanding of their family members' mental problems and were able to better support them when they had access to their EHR. Finally, policy stakeholders and experts addressed ethical challenges and recommended the development of guidelines and trainings to better prepare both clinicians and SUs on how to write and read notes.
Conclusions: PAEHRs in MHC may strengthen user involvement, patients' autonomy, and shift medical treatment to a coproduced process. Acceptance issues among health care professionals align with the findings from general health settings. However, the corpus of evidence on digital sharing of EHRs with people affected by mental health conditions is limited. Above all, further research is needed to examine the clinical effectiveness, efficiency, and implementation of this sociotechnical intervention.

15. Sleigh, J., and Vayena, E. (2021), Public engagement with health data governance: the role of visuality. Humanit Soc Sci Commun 8, 149 https://doi.org/10.1057/s41599-021-00826-6

Abstract

Over the last years, public engagement has become a topic of scholarly and policy debate particularly in biomedicine, a field that increasingly centres around collecting, sharing and analysing personal data. However, the use of big data in biomedicine poses specific challenges related to gaining public support for health data usage in research and clinical settings. The improvement of public engagement practices in health data governance is widely recognised as critical to address this issue. Based on OECD guidance, public engagement serves to enhance transparency and accountability, and enable citizens to actively participate in shaping what affects their lives. For health research initiatives, this provides a way to cultivate cooperation and build public trust. Today, the exact formats of public engagement have evolved to include approaches (such as social media, events and websites) that exploit visualisation mediated by emerging information and communication technologies. Much scholarship acknowledges the advantages of visuality for public engagement, particularly in information-dense and digital contexts. However, little research has examined how health data governance actors utilise visuality to promote clarity, understandability and audience participation. Beyond simply acknowledging the diversity of possible formats, attention must also be paid to visualisations' rhetorical capacity to convey arguments and ideas and motivate particular audiences in specific situations. This paper seeks to address this gap by analysing both the approaches and methods of argumentation used in two visual public engagement campaigns. Based on Gottweis' analytical framework of argumentative

performativity, this paper explores how two European public engagement facilitators construct contending narratives in efforts to make sense of and grapple with the challenges of health data sharing. Specifically, we analyse how their campaigns employ the three rhetorical elements logos, ethos and pathos, proposed by Gottweis to assess communicative practices, intermediated and embedded in symbolically rich social and cultural contexts. In doing so, we highlight how visual techniques of argumentation seek to bolster engagement but vary with rhetorical purposes, as while one points to health data sharing risks, the other focuses on benefits. Moreover, drawing on digital and visual anthropology, we reflect on how the digitalisation of communicative practices impacts visual power.

16. 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.

Abstract

This study explored the sociotechnical influences shaping the naturally-occurring adoption and non-adoption of device technologies in the UK's National Health Service (NHS), amid increasing policy interest in this area. The study was informed by Science and Technology Studies and structuration and Actor Network Theory perspectives, drawing attention to the performative capacities of the technology alongside human agentic forces such as agendas and expectations, in the context of structural and macro conditions. Eight technologies were studied using a comparative ethnographic case study design and purposive and snowball sampling to identify relevant NHS, academic and industry participants. Data were collected

between May 2009 and February 2012, included in-depth interviews, conference observations and printed and web-based documents and were analysed using constructivist grounded theory methods. The study suggests that while adoption decisions are made within the jurisdiction of healthcare organisations, they are shaped within a dynamic and fluid 'adoption space' that transcends organisational and geographic boundaries. Diverse influences from the industry, health care organisation and practice, health technology assessment and policy interact to produce 'technology identities.' Technology identities are composite and contested attributes that encompass different aspects of the technology (novelty, effectiveness, utility, risks, requirements) and that give a distinctive character to each. We argue that it is these socially constructed and contingent heuristic identities that shape the desirability, acceptability, feasibility and adoptability of each technology, a perspective that policy must acknowledge in seeking to intervene in health care technology adoption.

17. van Grunsven, J. (2021), Perceptual breakdown during a global pandemic: introducing phenomenological insights for digital mental health purposes. Ethics Inf Technol 23, 91–98 (2021). https://doi.org/10.1007/s10676-020-09554-y

Abstract

Online therapy sessions and other forms of digital mental health services (DMH) have seen a sharp spike in new users since the start of the COVID-19 pandemic. Having little access to their social networks and support systems, people have had to turn to digital tools and spaces to cope with their experiences of anxiety and loss. With no clear end to the pandemic in sight, many of us are likely to remain reliant

upon DMH for the foreseeable future. As such, it is important to articulate some of the specific ways in which the pandemic is affecting our self and world-relation, such that we can identify how DMH services are best able to accommodate some of the newly emerging needs of their users. In this paper I will identify a specific type of loss brought about by the COVID-19 pandemic and present it as an important concept for DMH. I refer to this loss as loss of perceptual world-familiarity. Loss of perceptual world-familiarity entails a breakdown in the ongoing effortless responsiveness to our perceptual environment that characterizes much of our everyday lives. To cash this out I will turn to insights from the phenomenological tradition. Initially, my project is descriptive. I aim to bring out how loss of perceptual world-familiarity is a distinctive form of loss that is deeply pervasive yet easily overlooked—hence the relevance of explicating it for DMH purposes. But I will also venture into the space of the normative, offering some reasons for seeing perceptual world-familiarity as a component of well-being. I conclude the paper with a discussion of how loss of perceptual world-familiarity affects the therapeutic setting now that most if not all therapeutic interactions have transitioned to online spaces and I explore the potential to augment these spaces with social interaction technologies. Throughout, my discussion aims to do justice to the reality that perceptual world-familiarity is not an evenly distributed phenomenon, that factors like disability, gender and race affect its robustness, and that this ought to be reckoned with when seeking to incorporate the phenomenon into or mitigate it through DMH services.

18. 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

Abstract

Aim: To explore current research on the ethics of smart home technologies including artificial intelligence and information technologies for elderly care by conducting a scoping review.

Background: The development of smart home technologies for care of the older adults provides potential solutions to reduce the caregiver burden within families where they are urgently needed. Building an ethical system to support the application of these technical products should be explored.

Methods: The literature search was performed in seven electronic databases. Relevant studies from January 2015 to February 2021 were selected; screening and analysis were completed independently by two researchers.

Results: There were a total of 15 included studies on the ethics of smart home technologies for elderly care, which focused on the following issues: privacy (information privacy and physical privacy), autonomy (independence, informed consent and user-centred control), safety guarantee, fairness and concerns about reduced human contact.

Conclusions: There exist a number of ethical conflicts in the application of smart home technologies for elderly care. Therefore, it is necessary to further investigate the ethical issues with regards to the decision-making process of weighing the advantages and disadvantages of these technologies.

Implications for nursing management: Efforts should be made to establish a corresponding ethical framework to ensure the sustainable development of smart, home-based elderly care. Nurses may play an important role in the design and implementation of these technologies to promote ethical awareness and practice.

*Children and Families*

1. Cooner, T. S., Beddoe, L., Ferguson, H. & Joy, E. (2020) The use of Facebook in social work practice with children and families: exploring complexity in an emerging practice, Journal of Technology in Human Services, 38:2, 137-158, DOI: 10.1080/15228835.2019.1680335

Abstract

This article draws from a 15-month participant observation study of social work and child protection practices in England to illustrate how social workers used Facebook to gain another view of service-users' lives. Social media use was not an intended focus for the study, its presence emerged during our data analysis. While some research has shown that such practices occur, our long-term ethnographic approach provides new insights into how Facebook was actually used in ongoing casework with families and why it was used. Our findings show that Facebook use took multiple forms. Some social workers actively searched service users' Facebook pages and some opposed any such usage. We further advance the literature by introducing a third group who were unwillingly "drawn into" acting on Facebook information presented to them by others such as their managers. Our research insights suggest that social work must pause to consider the implications of these complex emerging practices.

2. Egard, H., & Hansson, K., (2021) The digital society comes sneaking in. An emerging field and its disabling barriers, *Disability & Society*, DOI: 10.1080/09687599.2021.1960275

Abstract

This study examines disabled people's everyday experience of social exclusion in relation to the rapid growth of digital technologies in everyday practices. It highlights the relationships between the growing theoretical apparatus on how society changes with new digital technologies, and theories about how this might lead to new disabling barriers in the everyday lives of disabled people. To better understand disabled people's everyday experiences of social exclusion in the digital age, it brings together insights from two different fields: digital technology, mainly in digital social science and digital humanities; and disability studies, with a focus on the digital divide. The study draws on empirical observations, photographs and interviews with adults with various disabilities in Sweden, and analyses their everyday experiences with the help of a theoretical framework.

3. Gillingham, P., (2019), Developments in Electronic Information Systems in Social Welfare Agencies: From Simple to Complex, The British Journal of Social Work, 49, 1: 135–146, https://doi.org/10.1093/bjsw/bcy014

Abstract

The problems with current forms of electronic information systems (IS) being used by social welfare agencies have been documented by researchers internationally and attention is turning to how they might be better designed and used. In this article, drawing from ethnographic research about IS implementation and evaluation with a number of social welfare agencies, two different approaches—one simple and one complex—to designing and using IS in social welfare agencies are presented. The advantages and disadvantages of each approach, as emerged from discussions with research participants, are explored. The aim of the article is to assist both decision

makers and practitioners in social welfare agencies to clarify their needs in relation to how future IS are designed and used.

4. Jackson, N., & Burke, K. (2019). Attitudes to and experiences of genetic information and testing among professionals working in the context of adoption. Adoption & Fostering, 43(3), 256–273. https://doi.org/10.1177/0308575919864187

Abstract

In the process of creating a care plan or finding a placement for children, assessment of their health and developmental needs will be undertaken. This can involve the interpretation of complex family history information and may also include undertaking and interpreting the results of genetic testing, when within professional guidelines. This study explores opinions, knowledge about and experiences of adoption professionals in relation to genetic information and testing in Wales. Semi-structured qualitative interviews were conducted with six social workers and seven medical advisers. The data were transcribed and thematically analysed. Themes included the challenges to collation of family history, how the willingness of professionals to undertake genetic testing in children awaiting adoption was altered by the availability (and non-availability) of family history information, and the uncertainty that genetic information can generate for professionals and prospective parents. Uncertainty for both professional groups emerged from apparent inconsistency in current practice and from concern over their own lack of genetic knowledge. As new genetic technologies increase the scope of uncertainty, there is a need for social workers and medical practitioners working in adoption to have a

greater understanding of genetics alongside opportunities to discuss cases in a multidisciplinary setting when appropriate.

5. Mathiyazhagan, S. (2021), Field Practice, Emerging Technologies, and Human Rights: the Emergence of Tech Social Workers. J. Hum. Rights Soc. Work. https://doi.org/10.1007/s41134-021-00190-0

Abstract

Structural inequalities, historical oppression, discrimination, social exclusion, power, and privilege are some of the most pressing human rights issues that social workers deal with in everyday practice. In the recent past, all these issues are not only prevalent in offline communities, but they are also active in online communities. The digital divide and online polarizations perpetuate power and privilege within and outside of social work practice. Social work practices are moving beyond boundaries, expanding, and adopting emerging technologies in all aspects of social work education, research, and practice. This paper has been prepared based on my last decade of transnational social work practice experience and fieldwork supervision. There is an emerging need for tech social work practices in all fields of social work. This paper discusses the challenges and opportunities for tech social work in the field and explores a possible model for tech social work practice to support safe and inclusive communities on and offline to promote human rights.

6. Pink, S., Ferguson, H., & Kelly, L. (2022). Digital social work: Conceptualising a hybrid anticipatory practice. Qualitative Social Work, 21(2), 413–430. https://doi.org/10.1177/14733250211003647

Abstract

While the use of digital media and technologies has impacted social work for several years, the Covid-19 pandemic and need for physical distancing dramatically accelerated the systematic use of video calls and other digital practices to interact with service users. This article draws from our research into child protection to show how digital social work was used during the pandemic, critically analyse the policy responses, and make new concepts drawn from digital and design anthropology available to the profession to help it make sense of these developments. While policy responses downgraded digital practices to at best a last resort, we argue that the digital is now an inevitable and necessary element of social work practice, which must be understood as a hybrid practice that integrates digital practices such as video calls and face-to-face interactions. Moving forward, hybrid digital social work should be a future-ready element of practice, designed to accommodate uncertainties as they arise and sensitive to the improvisatory practice of social workers.

**Appendix 3: UK Case Law**

| UK Case Law | | | |
|---|---|---|---|
| **Citation** | **Topic** | **Key Facts/Issues** | **Findings/Relevant Judicial Reasoning** |
| AS1's (A Child) Application for Judicial Review, Re [2021] NIQB 11 | Retention of data (video footage) | Video footage taken by police of a search which captured images of a child in his home. | • Search conducted lawfully under terrorism legislation<br>• Data lawfully retained in accordance with the Police Service of Northern Ireland's policy.<br>• The footage had been relevant to possible criminal charges, a complaint to the Police Ombudsman and potential civil litigation and therefore met the test for retention. |
| BC and Others v Iain Livingstone QPM, Chief Constable of the Police Service of Scotland and Others, [2020] CSIH 61 | Queries the nature and scope of a common law right to privacy in Scotland similar in scope to the Article 8 ECHR right to privacy. | Petitioners were seeking a declarator that the respondents' use of messages sent to, from and amongst the reclaimers in private "WhatsApp" electronic message groups ("the Messages") to bring misconduct proceedings against | • **Lady Dorrian at para 83 "**The existence in Scotland of an obligation of confidence has long been recognised, and here too the need for a confidential relationship has given way to a focus on the knowledge of those possessing the information that it had been imparted in confidence (Lord Advocate v Scotsman Publications 1988 SLT 490). I see no reason to think that the effect of articles 8 and 10 in respect of this area of the law in Scotland is any different to that in England, but it does not mean that there has thereby |

| | | | |
|---|---|---|---|
| | | them in respect of allegations of non-criminal behaviour was unlawful et separatim incompatible with their ECHR article 8 rights | been created a widely applicable general right of privacy” |
| Excession Technologies Ltd v Police Digital Service 2022 WL 00597263 | Procurement process for computer and information systems. | Addressed the procurement process applicable to the appointment of a contractor to a framework agreement for the provision of computer and information technology services in respect of a covert surveillance operation room. | • PDS was entitled to rely on the exemption under regulation 7(1)(b) of Defence and Security Public Contracts Regulations 2011 in relation to the Procurement |
| HMA v Purves 2009 S.L.T. 969 | Validity of authorisation of directed surveillance by electronic means. | An accused was charged with being concerned in the supply of controlled drugs. At a | • Held that authorisation of directed surveillance via an secure online system met with the requirements that authorisation be in |

preliminary hearing, the accused lodged a minute against the admissibility of certain evidence which had been obtained by directed surveillance, authorisation for which had been granted by a police superintendent in terms of the Regulation of Investigatory Powers (Scotland) Act 2000 via a secure online system. The accused submitted that the authorisation was invalid as it was not a written document as required by s 19(1)(b) of the 2000 Act and failed to bear the superintendent's signature.

writing in terms of s19(1)(b) Regulation of Investigatory Powers (Scotland) Act 2000.

| | | | |
|---|---|---|---|
| L v HM Advocate [2014] HCJAC 35 | Admissibility of evidence obtained from interrogation of phone (following detention). | Appellants detained under s14 CPSA 1995.<br><br>Phone taken from one appellant and interrogated.<br><br>Appellants were charged with assault to injury and permanent disfigurement.<br><br>Preliminary issue raised re admissibility of evidence. | • Held that since the nothing more had to be done other than connect the device to a power source and touching portions of the screen this fell within the scope of a s14(7)CPSA1995 examination.<br>• There was some suggestion in the case that the position may be different where the device was internet enabled and linked to social media accounts suggesting that examination of those accounts may or may not fall within the scope of s14(7) depending on the security settings of those accounts. |
| R (on the application of Bridges) v Chief Constable of South Wales [2020] EWCA Civ 1058 | Trial of automated facial recognition software. | | Held,<br><br>• That in determining whether an interference with the rights guaranteed under article 8 of the Human Rights Convention was “in accordance with the law” within the meaning of article 8.2 , a relativist approach was to be adopted,<br><br>• The more intrusive the act complained of, the more precise and specific the law said to justify it was required to be;<br><br>• The interference complained of in the present case was not analogous to the taking of |

photographs or the use of CCTV cameras by the police but, rather, fell somewhere in between the two poles on a spectrum ranging from, on the one hand, the storing of photographs and intelligence notes on a database and, on the other hand, the retention of fingerprint and DNA samples; that, in particular it was relevant that (i) AFR was a novel technology, (ii) it involved the capture of images and processing of digital information of a large number of members of the public, the vast majority of whom were unlikely to be of interest to the police, (iii) the data concerned was “sensitive personal data” within the meaning of the Data Protection Act 2018 and (iv) the data was processed in an automated way;

- The framework governing the use of AFR by the defendant's police force, which comprised the 2018 Act, the Secretary of State's Surveillance Camera Code and the policy documents of the defendant's police force, was insufficient to constitute the “law” for the purposes of article 8.2 , since all that was required under that framework was that there had to be a proper law enforcement purpose and the deployment of AFR Locate had to be considered necessary to achieve that purpose; that that left two impermissibly wide

areas of discretion outside the scope of the governing framework, namely (i) the selection of those individuals who would be included on watch lists when AFR Locate was being deployed and (ii) the locations where AFR Locate might be deployed, for which no normative requirement was laid down;

- The interference with article 8 rights occasioned by the police force's past and continuing use of AFR Locate could not be justified under article 8.2.

- That in light of the finding that the use of AFR Locate was not “in accordance with the law” for the purposes of article 8.2 , the inevitable consequence was that, notwithstanding the attempt of the data protection impact assessment to grapple with the article 8 issues, it had failed properly to assess the risks to the rights and freedoms of data subjects and the measures envisaged to address the risks arising from the deficiencies, as required by section 64(3)(b) and (c) of the 2018 Act, because it had proceeded on the basis that article 8 had not been infringed

- That although the public sector equality duty in section 149 of the Equality Act 2010 was a duty of process and not outcome, that did not diminish its importance since good processes were more likely to lead to better informed, and therefore better, decisions, and helped to make public authorities accountable to the public;

- That the public sector equality duty, which was dependent on the context, required a public authority to take reasonable steps to make enquiries about what might not yet be known to it about the potential impact of a proposed decision or policy on people with the relevant characteristics, in particular for present purposes, race and sex; that whilst there was no evidence that AFR had any bias on racial or gender grounds, the whole purpose of the positive duty (as opposed to the negative duties in the 2010 Act) was to ensure that a public authority did not inadvertently overlook information which it ought to take into account;

- That before or during the course of a trial process it was all the more important for a public authority to acquire relevant

information in order to conform to that duty and, in particular, to avoid indirect discrimination on racial or gender grounds;

- That in the present case, the defendant's police force had never sought to satisfy themselves, either directly or by way of independent verification, that the software program did not have an unacceptable bias on grounds of race or sex; and that, accordingly, the police force had not done all that it reasonably could, prior to or in the course of its use of AFR Locate and on an ongoing basis, to discharge its non-delegable duty under section 149 of the 2010 Act (post, paras 176, 179–182, 199–201, 210). R (Elias) v Secretary of State for Defence [2006] 1 WLR 3213 , CA, R (Bracking) v Secretary of State for Work and Pensions (Equality and Human Rights Commission intervening) [2014] Eq LR 60 , CA and Hotak v Southwark London Borough Council [2016] AC 811 , SC(E) applied.

- Where a general measure is challenged on article 8 grounds, it is appropriate for the court, when determining whether the interference with the article 8 right is

| | | |
|---|---|---|
| R. (on the application of Business Energy Solutions Ltd) v Preston Crown Court [2018] EWHC 1534 (Admin) | Scope and applicability of the Criminal Justice and Police Act 2001 in relation to the requirement to return copied data (that had been copied from seized devices). | proportionate, to assess the balance between the impact on every person who is affected by the measure and the interests of the community. Where, however, the substance of the challenge is not a general measure but a very specific deployment of a measure on a particular occasion against a particular individual such a wide assessment is not appropriate (post, paras 140–143).<br><br>Held,<br><br>• Copied data is subject to a duty of return (as seized property). The Crown Court could instruct is destruction (subject to considerations of ‘reasonable practicability’.<br><br>• The reasonable practicability of separation test in section 53 of the 2001 Act, was not confined to physical or technical considerations which, while they might play a part in the analysis, were by no means the only criteria for assessment; that, having applied the correct test, the judge had been best placed to form a conclusion about the dispute before him and had been entitled to accept the authority's submissions that in order to comply with the claimants’ request it would have been required to divert very |

| | | |
|---|---|---|
| | | substantial human and manual resources to the task. |
| R (on the application of C) v Commissioner of Police of the Metropolis [2012] EWHC 1681 (Admin) | Retention of custody photographs (where charges are not pursued). | • Acknowledged that the retention of such photographs was a violation of Article 8(1) and that while s64A Police and Criminal Evidence Act 1984 was 'too broad and imprecise' taken together with the Code of Practice on the Management of Police Information and the Management of Police Information Guidance there was a clear and detailed framework governing the exercise of the discretion that ensured such retention was in accordance with the law.<br>*Held* ,<br>• That the state's systematic collection and storage in retrievable form of public information about an individual was an interference with private life such as to engage article 8.1 of the Convention and so required to be "in accordance with the law" within article 8.2 ; that such term was not limited to requiring an ascertainable legal basis for the interference as a matter of domestic law, but also ensured that the law was not so wide or indefinite as to permit interference with the right on an arbitrary or abusive basis; that, for that purpose, the rules |
| R (on the application of Catt) v Association of Chief Police Officers of England, Wales and Northern Ireland [2015] UKSC 9 | Judicial review proceedings in respect of data retention provisions relating to a "domestic extremism" database maintained by the National Public Order Intelligence Unit and separately the retention of warning notices. | |

in question did not need to be statutory, provided that they operated within a framework of law and that there were effective means of enforcing them, and provided that their application, including the manner in which any discretion would be exercised, was reasonably predictable, if necessary with the assistance of expert advice; that the retention of data in police information systems in the United Kingdom, being subject to the provisions of the Data Protection Act 1998 and to published administrative codes of practice issued pursuant to section 39A of the Police Act 1996 , as inserted, was in accordance with the law; and that, accordingly, that pre-condition having been met, the question was whether the collection and storage of the data in relation to the claimants in each case was proportionate to its objective of securing public safety or preventing disorder or crime, so as to be justifiable (post, paras 4, 6, 11-13, 17, 47-50, 58, 60).

- Allowing the appeal in the first case (Lord Toulson JSC dissenting), that the retention of data recording information relating to attendees of political protest meetings served a proper policing purpose (namely, of enabling the police to make a more informed assessment of the risks and the threats to

public order associated with demonstrations forming part of an identifiable campaign and of the scale and nature of the police response which might be necessary in future, to investigate criminal offences where there had been any, to identify potential witnesses and victims, and to study the leadership, organisation, tactics and methods of protest groups which had been persistently associated with violence, and other protest groups associated with them); that the fact that some of the information recorded in the database related to attendees who had not committed and were not likely to commit offences did not make it irrelevant for legitimate policing purposes but rather could be of importance not only for the prevention and detection of crime associated with public demonstrations, but to enable the great majority of public demonstrations which were peaceful and lawful to take place without incident and without an overbearing police presence; and that, accordingly, the police had shown that the retention of data in nominal records of other persons about the claimant's participation in demonstrations, albeit amounting to a minor interference with his right to private life, was justified under article 8.2 by the legitimate requirements of police intelligence-gathering in the interests of

the maintenance of public order and the prevention of crime (post, paras 7, 25-26, 29-31, 34, 35, 52, 56, 57-58, 60).

- Allowing the appeal in the second case, that a harassment letter issued pursuant to the Prevention of Harassment Act 1997 was intended to warn the recipient that some conduct on his or her part might, if repeated, constitute an offence and thus prevent the recipient from denying that he or she knew that it might amount to harassment, and as such served a legitimate policing function of preventing crime or bringing an accused to justice; that (Lord Neuberger of Abbotsbury PSC and Lord Sumption JSC dissenting in part) the standard practice of retaining material relating to potential harassment cases for seven or 12 years was proportionate, provided that it was flexible enough to allow for deletion when the information was no longer required; and that, accordingly, since the material relating to the claimant had been deleted after a few years when it was no longer required, the Court of Appeal had erred in finding its retention to be a disproportionate interference with her right to private life (post, paras 42, 44, 46, 54-56, 57, 59, 60, 76-77).

| | | | |
|---|---|---|---|
| | | 11 year old referred through prevent strategy. | • Breached his Article 8 right to private and family life and the Data Protection Act 2018 s35 and s39. |
| R. (on the application of II) v Commissioner of Police of the Metropolis [2020] EWHC 2528 (Admin) | Retention of data | Personal data retained.<br><br>Age 16 – challenging continued retention. | • Importantly it was held that a proportionality assessment under Article 8 would determine whether retention was “necessary” within the meaning of s35(2)(b) and s39(1) DPA 2018. |
| R (on the application of M) v The Chief Constable of Sussex Police, Brighton & Hove [2021] EWCA Civ 42 | Scope and application of Part 3 of the Data Protection Act 2018. | Claim for judicial review fell into two parts. The first was a challenge to the lawfulness of the Respondent's safeguards for disclosing sensitive personal data to the Brighton & Hove Business Crime Reduction Partnership ("the BCRP") under an Information Sharing Agreement made in December 2018 ("ISA 2018"). The second | • It found “what matters for the purposes of demonstrating compliance with section 42(2) of the DPA 2018 is the *substance* of the policy document relied on, and whether in circumstances where the data to be processed is or might be characterised as "special category" or "sensitive" data (as the case may be), the document (a) explains the controller's procedures for securing compliance with the data protection principles in respect of such data, and (b) explains the controller's policies as regards the retention and erasure of such data.” |

| | | | |
|---|---|---|---|
| | | part of the claim was a discrete complaint about the unlawfulness of specific past disclosures of M's personal data, including sensitive personal data, allegedly made by the Respondent to the BCRP. | |
| R (on the application of Miller) v College of Policing [2021] EWCA Civ 1926 | Recording of perception-based hate crime and Data Protection Act 2018. | Concerned perception-based recording of hate crime and the lawfulness of Hate Crime Operational Guidance. | • Affirmed that "no statutory authorisation is necessary in relation to non-intrusive methods of data collection, even where the gathering and retention of that data interferes with Convention rights".[129] That being said, it acknowledged that there would still be an obligation to abide by the Data Protection Act 2018 and the Human Rights Act 1998. |
| R (on the application of the National Council for Civil Liberties (Liberty)) v Secretary of State for the Home | Data retention following Investigatory | Judicial review proceedings seeking a declaration of incompatibility | *Held,* dismissing the claim,<br>• That the question of compatibility with the Convention was to be determined by |

[129] R (on the application of Miller) v College of Policing [2021] EWCA Civ 1926 at para 56.

| | | | |
|---|---|---|---|
| Department [2019] EWHC 2057 (Admin) | Powers Act 2016 warrants. | under section 4 of the Human Rights Act 1998 2 in respect of "Bulk interception warrants", "bulk equipment interference warrants", "thematic equipment interference warrants", "bulk personal dataset warrants", "bulk acquisition warrants" and the power to authorise any officer of the authority to obtain or retain communication data granted in terms of the Investigatory Powers Act 2016. | reference to the totality of the interlocking safeguards applicable at the various stages of the bulk interception process, rather than by reference to the potential breadth of the information that could in principle be retained under the bulk interception power;<br>• That the safeguards relevant to bulk interception warrants under Chapter I of Part 6 of the Investigatory Powers Act 2016 included<br>(i) the requirement that the Secretary of State could only issue such a warrant if he considered that it was necessary on one of the statutory grounds and that the conduct authorised by it was proportionate to what was sought to be achieved,<br>(ii) the requirement for approval by a judicial commissioner,<br>(iii) the requirement that a warrant application contain a description of the communications to be intercepted,<br>(iv) the narrowness of the definition of "overseas-related communications" which could be intercepted,<br>(v) the requirement that a warrant specify the operational purposes for which any intercepted content or secondary data obtained under the warrant might be selected for examination, |

(vi) the powers given to the Investigatory Powers Commissioner to oversee the whole interception process and

(vii) the fact that it was open to a person to complain or bring a claim under the Human Rights Act 1998 to the Investigatory Powers Tribunal;

- That those safeguards were sufficient to prevent the risk of abuse of discretionary power and so met the requirement in articles 8.2 and 10.2 of the Convention respectively that any interference with Convention rights was "in accordance with the law" and "prescribed by law";
- That, likewise, the safeguards that applied to bulk and thematic equipment interference warrants under Part 5 and Chapter 3 of Part 6 of the 2016 Act, bulk personal dataset warrants under Part 7 of the 2016 Act and bulk acquisition warrants under Chapter 2 of Part 6 of the 2016 Act, many of which were the same as or similar to those which applied to bulk interception warrants, were sufficient to meet the requirements of articles 8.2 and 10.2 ;
- And that, in light of the fact that the powers under Parts 3 and 4 of the 2016 Act were subject to the necessity and proportionality tests and, where necessary, were subject to approval by a judicial commissioner or the

Office for Communications Data, it could not be said that the purposes for which those powers could be exercised was too wide or arbitrary, or that Parts 3 and 4 were incompatible with the Convention rights on any other ground

- That when deciding whether to exercise powers relating to warrants and authorisations under Parts 3, 4, 5, 6 and 7 of the 2016 Act a public authority was required under section 2(2)(b) to have regard to whether the level of protection to be applied in relation to any obtaining of information by virtue of the warrant or authorisation was higher because of the particular sensitivity of that information;
- That, further, by virtue of section 2(5)(a) "sensitive information" included items subject to legal privilege; that, therefore, the need to treat legally privileged items as sensitive was a principle which suffused the entire regime in the 2016 Act;
- That Parts 5 and Chapters 1 and 3 of Part 6 of the Act also contained a wide range of dedicated and detailed safeguards for legally privileged items;
- That although those additional safeguards did not apply to all types of data, and no specific safeguards applied to the bulk acquisition of communications data, the general privacy

duties in section 2 and the relevant parts of the code of practice nevertheless applied;

- That neither Strasbourg nor domestic jurisprudence lay down a general requirement for prior independent authorisation of interference with lawyer-client communications in order to achieve compatibility with article 8 ;
- And that, accordingly, the rules regarding legally privileged items were set out in the 2016 Act and codes of practice with sufficient clarity and with sufficient safeguards so as to avoid arbitrary interference and so as to render the statutory scheme compatible with article 8 of the Convention.
- That since by section 2(5)(b) of the 2016 Act "sensitive information" included any information identifying or confirming a source of journalistic information, section 2 also protected confidential journalistic material; that, moreover, additional safeguards applied in the case of a targeted warrant for interception or examination, requiring prior approval by a judicial commissioner (or any other person independent of the executive) and consideration of questions of necessity and proportionality;
- That although bulk warrants under Part 6 of the 2016 were not subject to similar safeguards, there was no requirement under

the Convention for prior independent authorisation where information was obtained in bulk and was then searched in order to identify a source or to obtain journalistic material; and that, accordingly, the provisions of the 2016 Act were not incompatible with article 10 of the Convention in so far as it was suggested that there were inadequate protections for confidential journalistic material.

- That the question whether and to what extent the Security Service had complied with the requirements of the law did not provide a basis for making a declaration of incompatibility in respect of the 2016 Act; that, in any event, it had not been established that the evidence proved that the safeguards created by the 2016 Act were insufficient to prevent abuse of the powers under challenge;
- That, rather, the fact that defects had now been identified in the handling arrangements on the part of the Security Service indicated that the system was in truth capable of preventing abuse;
- And that, accordingly, a declaration of incompatibility would be refused (post, paras 354, 387-390, 399).

| | |
|---|---|
| R (on the application of Wood) v Commissioner of Police of the Metropolis [2009] EWA Civ 414 | Retention of photographs |

*Privacy International v Secretary of State for Foreign and Commonwealth Affairs [2018] UKIPTrib IPT_15_110_CH* applied.

Held,

- That, although the mere taking of photographs of a person in a public place was not capable of engaging his rights under article 8(1) of the Convention, where a state authority such as the police visibly and with no obvious cause chose to take and retain photographs of an individual going about his lawful business in the street that was a sufficient intrusion by the state into the individual's privacy as to amount to a prima facie violation of his rights under article 8(1) ;
- That the taking and retention of the photographs of the claimant were in pursuance of a legitimate aim, namely “the prevention of disorder or crime”, or “the protection of the rights and freedoms of others”, for the purposes of article 8(2);
- And that the question whether that interference with the claimant's rights under article 8(1) was proportionate to the legitimate aim being pursued, so as to be justified as necessary in a democratic society, was a fact-sensitive question.

- Allowing the appeal (Laws LJ dissenting), that the required justification for the retention by the police of photographs of an individual had to be the more compelling where the interference with his rights was in pursuit of the protection of the community from the risk of public disorder or low level crime, as opposed to protection against the danger of terrorism or really serious criminal activity;
- That it was for the defendant to justify the interference with the claimant's article 8 rights as proportionate; that, in the circumstances, he had failed to do so; and that, accordingly, the interference with the claimant's rights was not justified under article 8(2).

- Of particular significance, Lord Collins of Mapesbury made the point that “it is plain that the last word has yet to be said on the implications for civil liberties of the taking and retention of images in the modern surveillance society.” And suggested that there is a need for “exploration of the wider, and very serious, human rights issues which arise when the State obtains and retains the images of persons who have committed no

| | | | |
|---|---|---|---|
| | | | offence and are not suspected of having committed any offence."[130] |
| Sutherland v HM Advocate for Scotland, [2020] UKSC 32 | Evidence procured by private individual passed to police – whether Article 8 violation. | Concerned the use of evidence procured by a paedophile hunter group that was subsequently passed to the police. | • Held that there was no Article 8 violation as there was no reasonable expectation of privacy in the communications because the communications themselves did not fall within the scheme of values the ECHR seeks to protect and promote.[131] |
| Young v HM Advocate [2013] HCJAC 145 | Admissibility of expert evidence on case linkage analysis. | Appellant convicted of several charges - all but one involved violence against women. One was a murder charge.<br><br>The Moorov doctrine was applied.<br><br>Later, the appellant was contacted in | • Held<br>1. That expert evidence might be admissible but the evidence had to be based on a recognised and developed academic discipline, following a developed methodology, and produce a result which was capable of being assessed and given more or less weight in light of all the evidence.<br>2. That at this point in time case linkage analysis need not possess the necessary qualities. |

[130] R (on the application of Wood) v Commissioner of Police of the Metropolis [2009] EWA Civ 414 at para 100.

[131] This decision has been subject to academic criticism on the basis that it is opens the door to covert surveillance for law enforcement purposes with the illusion of boundaries between private and state interference. See Allison M Holmes, Citizen led policing in the digital realm: paedophile hunters and article 8 in the case of Sutherland v Her Majesty's Advocate, M.L.R. 2022, 85(1), 219-231.

| | | | |
|---|---|---|---|
| | | relation to an investigation that was being carried out in relation to murders of six women including the appellants victim. This investigation was in part supported by case linkage analysis. | |
| | | Appellant argued that this new evidence would affect the jury's determination and that there had been a miscarriage of justice. | |
| Z (Children) (Application for Release of DNA Profiles), Re [2015] EWCA Civ 34 | DNA profiles and data sharing. | Concerned the question of the circumstances in which DNA profiles obtained by the police in exercise of their criminal law enforcement functions can, without the consent of the data subject, be put | • Held, that, whether by applying a purposive approach to statutory interpretation or by interpreting the provisions in accordance with section 3 of the Human Rights Act 1998 in a way which was compatible with article 8 of the Convention, on a true construction section 22 of the Police and Criminal Evidence Act 1984 did not permit the police to retain and use biometric material seized under section 19 for any other purpose than criminal law enforcement; that the |

to uses which are remote from the field of criminal law enforcement.

commissioner therefore had no statutory power to retain and use the Part II sample other than for criminal law enforcement, and so could not disclose it for any other purpose; and that, accordingly, since the court could not exercise its inherent jurisdiction to require him to do something contrary to statute, the court could not order the commissioner to disclose the DNA profiles for use in care proceedings (post, paras 35–46, 49, 50, 54).

*Ghaidan v Godin-Mendoza [2004] 2 AC 557, HL(E)* and S v United Kingdom (2008) 48 EHRR 1169, GC applied.

*Per* McFarlane and Beatson LJJ. Since the issue is confined to biometric material seized from “premises” under Part II of the 1984 Act, the court's construction of Part II , aligning it with Part V , represents an exception confined to biometric material as distinct from any other form of material which may be seized by police from premises under Part II , and has no impact on the established arrangements for disclosure of Part II material other than biometric material (post, paras 51, 53).

**Appendix 4 International Case Law**

| International Case Law | | | |
|---|---|---|---|
| **Citation** | **Topic** | **Key Facts/Issues** | **Findings/Relevant Judicial Reasoning** |
| Breyer v Germany (2020) 71 E.H.R.R. 17 | Data sharing/access | Concerned the retention of telecommunications data that could be accessed by Law Enforcement. | The Court acknowledged that "where there has been a compilation of data on a particular individual, the processing or use of personal data or publication of the material concerned in a manner or degree beyond that normally foreseeable, private life considerations arise. Article 8 of the Convention thus provides for the right to a form of informational self-determination, allowing individuals to rely on their right to privacy as regards data which, albeit neutral, are collected, processed, and disseminated collectively and in such form or manner that their art.8 rights may be engaged."[76]<br><br>The Court made clear that the storage of information that relates to an individual's private life is an interference within the scope of Article 8(1). However, the question that then has to be |

answered is whether that interference is justified in terms of Article 8(2). In order for it to be justified it would have to be in accordance with the law, pursue a legitimate aim and be necessary and proportionate.[77]

In order to be 'in accordance with the law' "it is essential to have clear, detailed rules governing minimum safeguards concerning amongst other things duration, storage, usage, access of third parties, procedures for preserving the integrity and confidentiality of data and procedures for its destruction."[78]

Further, "an interference will be considered "necessary in a democratic society" for a legitimate aim if it answers a "pressing social need" and if it is proportionate to the legitimate aim pursued. The Court finds that the fight against crime, and in particular against organised crime and terrorism, which is one of the challenges faced by today's European societies, upholding public safety and the

| | | | |
|---|---|---|---|
| | | | protection of citizens constitute "pressing social needs". It also recognises that modern means of telecommunications and changes in communication behaviour require that investigative tools for law enforcement and national security agencies are adapted."[79] |
| Big Brother Watch v United Kingdom (58170/13) [2018] 9 WLUK 157 | The Regulation of Investigatory Powers Act for the bulk interception of electronic communications by UK security services did not contain adequate safeguards | | |
| Centrum for Rattvisa v Sweden (35252/08) [2018] 6 WLUK 691 | Interception of communications | Under Article 8 of ECHR, Centrum för Rättvisa (a Swedish non-profit) complained that the Swedish state practice and legislation concerning signals intelligence had violated and continued to violate its right to respect for private life and correspondence. | Held<br>Complaint dismissed.<br>The court was aware of the potentially harmful effects that the operation of a signals intelligence scheme could have on the protection of privacy. Nevertheless, it remained important to bear in mind the importance for national security operations. Court took into consideration the threat of terrorism/serious cross-border crime/communication technology; yet the decision to |

set up a bulk interception regime to identify such threats fell within the state's margin of appreciation. When examining the Swedish system of signals intelligence in abstracto, the court had had regard to the relevant legislation and the other information available in order to assess whether, on the whole, there were sufficient minimum safeguards in place to protect the public from abuse. While there were some areas where there was scope for improvement, notably the regulation of the communication of personal data to other states and international organisations and the practice of not giving public reasons following a review of individual complaints, the system revealed no significant shortcomings in its structure and operation.
The scope of the signals intelligence measures and the treatment of intercepted data were clearly defined in law, the authorisation procedure was detailed and entrusted to a judicial body and there were

| | | | |
|---|---|---|---|
| | | | several independent bodies tasked with the supervision and review of the system. Overall, and having regard to the margin of appreciation enjoyed by the national authorities in protecting national security, the Swedish system of signals intelligence provided adequate and sufficient guarantees against arbitrariness and the risk of abuse. The relevant legislation met the "quality of law" requirement and the "interference" established could be considered as being "necessary in a democratic society". Further, the structure and operation of the system were proportionate to the aim sought to be achieved. There had therefore been no breach of art.8 (see paras 179-181 of judgment). |
| Gaughran v United Kingdom (45245/15) [2020] 2 WLUK 607 | Indefinitely retention of DNA/fingerprints/photograph after recordable offence conviction. | According to legislation, the applicant's conviction was spent after five years. However, the policy of the Police Service of Northern Ireland (PSNI) was to retain indefinitely DNA profiles/fingerprints/photograph of any individual convicted of a recordable offence. The | The Court found that the retention of the applicant's DNA profile, fingerprints, and photograph amounted to an interference with his private life<br>The Court considered that most member States had regimes with time limits for retaining |

applicant claimed that this policy amounted to a disproportionate interference with the right to respect for his private and family life under article 8 and could not be justified.

biometric data of convicted persons. The UK was one of the few Council of Europe jurisdictions to permit indefinite retention of DNA profiles.

What was decisive was the existence and functioning of safeguards. The State had put itself at the limit of its margin of appreciation. So, it had to ensure that certain safeguards were effective for the applicant.

The applicant's biometric data and photographs had been retained without reference to the seriousness of his offence and without regard to any continuing need to retain that data indefinitely. Therefore the applicant could not request a review of the retention of his data, as there was no provision permitting erasure.

The Court found that the nature of those powers failed to strike a fair balance between the competing public and private interests.

The respondent State had therefore overstepped the

| | | | |
|---|---|---|---|
| | | | acceptable margin of appreciation and the retention at issue constituted a disproportionate interference with the applicant's right to respect for private life, which could not be regarded as necessary in a democratic society. There had accordingly been a violation of Article 8 of the Convention. |
| Khan v United Kingdom (35394/97) [2000] 5 WLUK 326 | Improperly obtained evidence from a secret listening device | Following a conviction of drug-dealing based on improperly obtained evidence from a secret listening device installed by the police. Appeal against conviction was dismissed on the ground that the invasion of his privacy was outweighed by the aim of proving he had been involved in serious crime. Complaints concern right to a fair trial was unfair, in breach of Article 6. | Held There had been a violation of Art.8 and Art.13 of the Convention. The interference was found not to be "in accordance with the law". The national rules were only outlined in the non-statutory Home Office Guidelines and therefore the domestic law did not give protection against interference with an individual's rights. It was not the ECHR's role to determine whether the evidence was admissible, and it found that the secretly taped evidence did not render the proceedings wholly unfair, as the domestic courts could have used their discretionary powers to exclude |

| | | | |
|---|---|---|---|
| | | | the evidence under the Police and Criminal Evidence Act 1984 s.78. The criminal proceedings did not provide a suitable remedy or protection from abuse, as the only body to which he could complain about the police surveillance was the Police Complaints Authority (PCA). The ECHR found such an investigation would be insufficiently impartial and therefore Art.13 was also breached. |
| Liberty v United Kingdom (58243/00) [2008] 7 WLUK 25 | Communications data/interception of communication | Civil liberties organisations alleged that between 1990 - 1997 their telephone and electronic communications had been intercepted by the Ministry of Defence. In domestic proceedings, no contravention of the Interception of Communications Act 1985 had been found. The organisations appealed to the ECHR. | Held<br>Complaint upheld.<br>(1) Legislation allowed secret monitoring of communications, which posed a threat of surveillance for all those to whom the legislation might be applied. Accordingly, there had been an interference with art.8.<br>(2) Section 3(2) of the 1985 Act allowed the authorities broad discretion to intercept communications between the United Kingdom and an external receiver. There was no limit to the type of external communications that could be included in a warrant under |

| | | | |
|---|---|---|---|
| | | | s.3(2). In principle, any person who sent or received telecommunications outside the British Islands during the period in question could have had their communication intercepted under a s.3(2) warrant. The details of safeguards/arrangements under s.6 of the 1985 Act were not contained in legislation or otherwise made available to the public. The domestic law did not set out in a form accessible to the public the procedure for examining, sharing, storing, and destroying intercepted material. The interference with the applicant's rights was not in in accordance with the law. Accordingly, art.8 had been violated. |
| Peck v United Kingdom (44647/98) [2003] 1 WLUK 607 | Disclosure of CCTV footage/photographs | The applicant was captured on CCTV with a knife and attempting suicide. The police stopped him from causing himself fatal harm. The CCTV footage was subsequently released to the press to demonstrate the effectiveness of CCTV. The applicant complained that his right to | Held<br>Upholding the complaint<br>No relevant or reasons which justified the local authority's disclosure. The local authority should have sought the applicant's consent, masked his identity, or ensured that the media had masked their identity. |

| | | | |
|---|---|---|---|
| | | private life under Article 8 ECHR had been breached by the disclosure of the CCTV footage by the local authority. He also complained a breach of Article 13 ECHR which requires the right to an effective remedy. | There were not sufficient safeguards in place to prevent the applicant's identity. The disclosure had been a disproportionate and unjustified interference with P's private life and accordingly infringed his Art.8 right.<br>There had been a violation of P's right under Art.13 as the applicant was not provided with an effective remedy for the breach of his Art.8 right. |
| Perry v United Kingdom (63707/00) [2003] 7 WLUK 485 | Covert videotaping by police/code of practice pursuant to PACE 1984 | The applicant was convicted of robbery and sentence to five years' imprisonment. The complaint was based on the use of covert videotaping for the purpose of identification in his prosecution. The applicant complained that his right to respect for private life had been violated. | Held<br>Upheld the complaint<br>Art.8 had been violated because the applicant did not know that he was being filmed when he went to the police station. Police did not comply with PACE, which led to an unlawful interreference with Art.8 as the individual was not informed that he was being filmed or obtained with this consent. |
| PG v United Kingdom (44787/98) [2001] 9 WLUK 349 | Covert surveillance/consent | The police installed a covert listening device at a flat after receiving information about an armed robbery and, although that robbery was abandoned. Listening devices were also used at the police station to | Held, allowing the application in part<br><br>(1) the utilisation by the police of the covert listening devices in the flat and in the police, station |

compare the applicants' voices with those recorded at the flat.
The applicants' complained that the use of the surveillance devices had infringed the right to respect for private life under and the right to an effective remedy. The case also involved the failure to disclose part of a report, and the use at trial of taped evidence procured by means of covert surveillance, had violated the right to a fair trial.

had breached Art.8(2) of the Convention.
(2) Obtaining information regarding the use of a telephone during the investigation of a conspiracy to commit armed robbery was justified under Art.8(2).
(3) The domestic courts were not able to provide an effective remedy pursuant to Art.13; the complaints investigation procedures did not meet the requisite levels of independence to provide protection against the abuse of authority, and thus the right to an effective remedy had been infringed.
(4) Article 6 had not been breached in respect of the non-disclosure as sufficient safeguards had been taken to protect the applicants' interests
(5) there was no unfairness in leaving the taped evidence to the jury as a thorough summing up had been provided.
(6) The method by which the voice samples had been obtained had not infringed the applicants' right not to incriminate themselves; voice

| | | | |
|---|---|---|---|
| | | | samples that did not include incriminating evidence were akin to physical samples, such as hair, to which the right did not apply. |
| RE v United Kingdom (62498/11) [2015] 10 WLUK 707 | Covert surveillance/code of practice | The regime for the covert surveillance of consultations between detainees and their lawyers and appropriate adults, set out in the Regulation of Investigatory Powers Act 2000 and the revised Covert Surveillance Code of Practice (the Revised Code), was in breach of ECHR art.8 | Held<br>Complaint upheld in part.<br>The main issue was whether the regime was "in accordance with the law" under art.8(2). The requirement that any interference had to be "in accordance with the law" would only be met when three conditions were satisfied. It was not in dispute that the surveillance regime had a basis in domestic law, namely the 2000 Act and the Revised Code of Practice. Moreover, both were public documents. Accordingly, the relevant domestic law was adequately accessible for the purposes of art.8. In the special context of secret surveillance measures, the instant court had previously found that "foreseeability" required that domestic law be sufficiently clear to give citizens an adequate indication as to the circumstances in which and the |

conditions on which public authorities were empowered to resort to any such measures. As to the covert surveillance of lawyer/client consultations, the instant court was not satisfied that the provisions in Pt II of the 2000 Act and the Revised Code concerning the examination, use and storage of the material obtained, the precautions to be taken when communicating the material to other parties and the circumstances in which recordings might or had to be erased or the material destroyed provided sufficient safeguards for the protection of the material obtained by covert surveillance. To that extent, during the relevant period of the applicant's detention in May 2010, the impugned surveillance measures, insofar as they might have been applied to him, did not meet the requirements of art.8(2). There had therefore been a breach of art.8. The position in relation to the covert surveillance of consultations between detainees and their appropriate adults was different:

| | | |
|---|---|---|
| S v United Kingdom (30562/04); Retention of DNA/fingerprints Marper v United Kingdom (30566/04) [2008] 12 WLUK 117 | The applicants complained that the retention by the authorities of their fingerprints/ cellular samples/DNA profiles after criminal proceedings against them had resulted in acquittal or been discontinued violated their rights under the article 8 of the ECHR. | the relevant provisions were accompanied by adequate safeguards against abuse and were not therefore in breach of art.8 (see paras 119-122, 141-143, 167-168 of judgment).<br>Cellular samples contain personal information, which means that their retention must be seen as interfering in one's private life.<br>DNA profiles can identify relationships between individuals, which can therefore interfere with the right to private lives of individuals of others.<br>The retention of cellular samples and DNA profiles, therefore, leads to an interference with the applicants' right to respect for their private lives, within the meaning of Article 8 of the Convention.<br>The retention of fingerprints also constitutes an interference with the right to respect for private life.<br>Other countries have chosen to set limits on the retention and use of such data with a view to achieving a proper balance with |

| | | | |
|---|---|---|---|
| | | | the interests of respecting individuals' private lives.<br>The court finds that there is a blanket and indiscriminate nature of the power of retention in England and Wales.<br>The retention of unconvicted people's data may be especially harmful in the case of minors, given their situation and the importance of their development and integration in society. |
| Recklos v Greece (1234/05) [2009] 1 WLUK 145 | Photograph/Consent | The applicants complained that that the taking of a photograph of their baby in hospital breached their rights under art.8 of the Convention. | Held<br>Complaints upheld.<br>(2) The right to protection of one's image was an essential part of personal development and presupposed the right to control the use of that image. This issue included the right to object to the reproduction of the image. Also, effective protection of an image presupposed obtaining the consent of the person at the time the picture was taken. The photographer did not have consent to take pictures of the baby, and consent was indispensable to establish the context in which the picture was to be used. |

| | | | |
|---|---|---|---|
| Szabo v Hungary (37138/14) [2016] WLUK 80 | Covert surveillance | In potential breach of Article 8, the applicants complained that they could potentially be subjected to unjustified and disproportionately intrusive measures within the Hungarian legal framework on secret surveillance for national security purposes. They allege that the legal framework was prone to abuse, notably for want of judicial control. They also complained that their exposure to secret surveillance without judicial control or remedy breached their rights under Article 6 and Article 13. | There had been a violation of art.8.<br>Held<br>Complaint upheld.<br>(1) Even though the applicants had not been subjected to surveillance, they could claim to be victims of a violation of their art.8 rights by virtue of the mere existence of the legislation. (see paras 38-39 of judgment).<br>(2) The legislation did not provide safeguards which were sufficiently precise, effective, and comprehensive on the ordering, execution, and potential redressing of surveillance measures. The scope of the measures could include virtually anyone. There was also a lack of judicial control. Judicial control offered the best guarantees of independence, impartiality, and a proper procedure.<br>There was an absence of effective remedial measures for those who were subject to surveillance measures. In the circumstances, the legislation was in breach of art.8 (paras 75, 77, 89). |

| | | |
|---|---|---|
| Tele2 Sverige AB v Post- och telestyrelsen (C-203/15) C:2016:970 | Data protection/retention of data | Members States may not impose a general obligation to retain data on providers of electronic communications services. Only targeted retention of that data may be allowed for the purpose of fighting serious crime. |

## Appendix 5: Legislation Table

The table below outlines the most relevant provisions from eight different pieces of legislation, which may apply to one or more of the emerging technologies discussed in this report.

The legislation is listed on the left side of the table.

Before each new piece of legislation begins, a row of six categories can be found. These subheadings should be read from left to right as the columns build on from the previous. The order of the subheadings can be described as follows:

(1) a signpost to the numbered section of the relevant act;

(2) a description of its contents;

(3) an outline of the main legislative clauses;

(4) the potential emerging technology to which it may be applied;

(5) a reference to any relevant case law; and

(6) findings and significance of that case law.

| Legislation | Section | Description | Summary | Applicable Emerging Technology | Applicable Case Law | Case Law Findings |
|---|---|---|---|---|---|---|
| Data Protection Act 2018 | 3(2) | Definition of “personal data” | Information relating to an identified or identifiable living individual | Databases<br><br>Biometric identification systems<br><br>Electronic surveillance Systems | | |
| DPA 2018 | 3(4) | Definition of “processing” | Operation performed on personal data, including collection, recording, organisation, structuring, storage, retrieval, use, disclosure by transmission, dissemination | Databases<br><br>Biometric<br><br>Surveillance | | |

| | | | | |
|---|---|---|---|---|
| | | | and making available. | |
| DPA 2018 | 33(4) | Definition of “profiling” | Profiling is a form of automated processing of personal data to analyse or predict qualities about an individual. | Database<br><br>Biometric<br><br>Surveillance |

| | | | | | | |
|---|---|---|---|---|---|---|
| DPA 2018 | 34-40 | Data protection principles | The principles under Part 3, Chapter 2, of the DPA are the provisions for processing personal data for a law enforcement purpose. | Databases<br><br>Biometric<br><br>Surveillance | R (Bridges) v Chief Constable of South Wales Police (Respondent) and others [2020] EWCA Civ 1058 | The police force had not satisfied the requirements of the first data protection principle in s.35 of the 2018 Act, namely that data processing had to be lawful and fair. |
| | | | | | Catt v. the United Kingdom | The Court emphasised the risk of ambiguity in the legal basis used by the authorities for the collection and retention of personal data, stemming from loosely defined notions in domestic law (paras 97 and 106). |
| DPA 2018 | 35(8) | Definition of “sensitive processing” | Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade | Databases<br><br>Biometric | Catt v. the United Kingdom | Data revealing political opinions are regarded as a “sensitive” category of personal data and, in the Court’s view, it is unacceptable for the national authorities to disregard this aspect by processing such data in |

| | | | | | |
|---|---|---|---|---|---|
| | | | union membership, genetic data, biometric data, and data concerning health or a person's sex life or sexual orientation. | Surveillance | accordance with ordinary domestic rules, without taking account of the need for heightened protection. The Court found a violation of Article 8, pointing out that the sensitive nature of the data in question should have constituted a key element of the case before the domestic courts, as it was before the Court (para 112). |
| DPA 2018 | 38(3) | The fourth data protection principle: personal data must be accurate and kept up to data. | Requires distinct categories to be made when processing personal data between data subjects, such as suspects, convicted persons, victims, and witnesses. | Databases<br><br>Biometric<br><br>Surveillance | |

| | | | | | | |
|---|---|---|---|---|---|---|
| DPA 2018 | 42 | Safeguards: sensitive processing | Section 35 requires controllers to have an appropriate policy document in place, which explains procedure for complying with DPA principles and the policies for retention and erasure of personal data. These provisions are reliant on consent of data subject or a condition in Schedule 8 | Databases<br><br>Biometric<br><br>Surveillance | AS1's (A Child) Application for Judicial Review, Re [2021] NIQB 11 | The interference was proportionate given the valid basis for the material's retention and there was an adequate system of review in place for the category of material. The 2018 Act provided a remedy for erasure of the footage |
| | | | | | R (Bridges) v Chief Constable of South Wales Police (Respondent) and others [2020] EWCA Civ 1058 | The court had held the processing to be "sensitive processing" within s.35(5), which meant that the defendant had to have an "appropriate policy document in place" meeting the requirements of s.42. The court found that the question of whether an appropriate policy document was in place did not need to be determined because the two deployments of AFR in the instant case occurred before the Act came into force (paras 155-161). |
| DPA 2018 | 45 | Data subject's right of access | The information that can be disclosed to a data subject on | Databases | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | request. Subsection (4) sets out grounds to refuse data subject's access either wholly or partly. | | | |
| DPA 2018 | 46-48 | Data subject's rights to rectification or erasure | Data subject can request data to be corrected, erased or processing to be restricted. The controller can restrict right to rectification if this request would obstruct an investigation. If request has been refused, data subject must be informed. | Databases | Catt v. the United Kingdom | The lack of effective safeguards to ensure the destruction, in a police database, of personal information disclosing the political opinions of a peaceful protester, once its retention became disproportionate, had entailed a violation of Article 8. |
| | | | | | Catt v. the United Kingdom | The deletion of data from a database in which it had been stored for police purposes was not particularly burdensome (para 127) |
| DPA 2018 | 49-50 | Right not to be subject to automated | Automated decision-making mut have a legal | Databases | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | decision-making | basis. A "significant decision" in this section means one that produces an adverse legal effect for the data subject or affects the data subject significantly. | Biometric<br><br>Surveillance | | |
| DPA 2018 | 55(3) | Controller requirements for implementing appropriate technical and organisation measures | Controller requires knowledge about the latest developments in technology; the nature, scope, context, and purpose of processing; and the potential risks to rights and freedoms from processing. | Databases<br><br>Biometric<br><br>Surveillance | Business Crime Reduction Partnership [2021] EWCA Civ 42 | Guidance about what constitutes "appropriate technical and organisational measures" in the context of law enforcement processing. |
| DPA 2018 | 64 | Data protection | DPIAs have statutory status, | Databases | R (Bridges) v Chief | The court had been wrong to find that the DPIA was adequate. AFR |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | impact assessment | which are required to highlight and address privacy concerns and risks to individuals' rights and freedoms. DPIAs must include provisions outlined in subsection (3). | Biometric<br><br>Surveillance | Constable of South Wales Police (Respondent) and others [2020] EWCA Civ 1058 | involved impermissibly wide areas of discretion. The DPIA failed to properly assess the rights and freedoms of data subjects and failed to address the measures envisaged to mitigate the risks arising from the identified deficiencies, as required by s.64(3)(b) and ( c) (paras 14, 151-154). |
| DPA 2018 | 73-78 | Transfers of personal data to third Countries etc | Ss.73-76 deals with general conditions for such transfers.<br><br>S77 outlines special conditions for recipients other than relevant authorities.<br><br>S78 details special provisions for subsequent | Databases | Elgizouli (Appellant) v Secretary of State for the Home Department (Respondent) [2020] UKSC 10 | Although there was no established common law principle which prohibited the sharing of information relevant to a criminal prosecution in a country which had not abolished the death penalty, the transfer did not meet the requirements for transfer of personal data to a third country as set out in the data Protection Act 2018, s.73. |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | transfer of personal data. | | | |
| | Section | Description | Summary | Applicable Emerging Technology | Applicable Case Law | Case Law Findings |
| Scottish Biometric Commissioner Act 2020 | 2 | Functions | The general function is to support and promote the adoption of lawful, effective, and ethical practices in relation to the acquisition, retention, use and destruction of biometric data by Police Scotland, the SPA, and the PIRC. | Biometric Identification Systems | | |
| Scottish Biometric Commissioner Act 2020 | 7 | Code of Practice | Commissioner must prepare and revise a code of practice on the acquisition, | Databases<br><br>Biometric Identification Systems | | |

| | | | | |
|---|---|---|---|---|
| | | | retention, use and destruction of biometric data for criminal justice and police purposes. Subsection (2) requires that the code of practice must include provision about when biometric data must be destroyed in cases where a relevant enactment does not make such provision | |
| Scottish Biometric Commissioner Act 2020 | 8 | Key considerations in preparing the code | In preparing the code, commissioner must have regard to human rights; individual's privacy; public's confidence in police handing | Databases<br><br>Biometric Identification Systems |

| | | | | |
|---|---|---|---|---|
| | | | biometric data; and safety of society. | Electronic Surveillance Systems |
| Scottish Biometric Commissioner Act 2020 | 20 | Reports & recommendations | Reports may include recommendations in relation to the technology used or capable of being used for the purpose of acquiring, retaining, using, or destroying biometric data | Databases<br><br>Biometric Identification Systems<br><br>Electronic Surveillance Systems |
| Scottish Biometric Commissioner Act 2020 | 34 | Meaning of “biometric data” | Information about an individual’s physical, biological, physiological, or behavioural characteristics which may reveal the identity of an individual, either on its own or when combined | Biometric Identifiable Systems<br><br>Electronic Surveillance Systems |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | with other information of a biometric or non-biometric nature. | | | |
| | Section | Description | Summary | Applicable Emerging Technology | Applicable Case Law | Case Law Findings |
| Police and Fire Reform (Sc) Act 2012 | 3(b) | Maintenance of the police | The Authority may provide and maintain equipment information technology systems if it is necessary for police functions. | Databases<br><br>Biometric Information Systems<br><br>Electronic Surveillance Systems | | |
| Police and Fire Reform (Sc) Act 2012 | 31 | Forensic Services | The Authority must provide forensic services to the Police Service, the Police Investigations and Review Commissioner | | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | and the Lord Advocate and procurators fiscal. | | | |
| Police and Fire Reform (Sc) Act 2012 | 32 | Policing principles | The policing principles are that the main purpose of policing is to improve the safety and well-being of persons, localities, and communities in Scotland, and that the Police Service, working in collaboration with others where appropriate, should seek to achieve that main purpose by policing in a way which is accessible to, and engaged | Databases<br><br>Biometric Identification Systems<br><br>Electronic Surveillance Systems | BC and Others v Iain Livingstone QPM, Chief Constable of the Police Service of Scotland and Others, [2020] CSIH 61 | Disclosure of information would not be arbitrary but would be dictated by consideration of the relevant policing standards and breaches thereof (paras 101-112, 131-132) |

| | | | | |
|---|---|---|---|---|
| | | | with, local communities, and promotes measures to prevent crime, harm, and disorder. | |
| Police and Fire Reform (Sc) Act 2012 | 87(8) | Provision of other goods and services | The Authority may provide goods and services to any other public body or office-holder, such as information technology systems and equipment (and services involving the development, provision, procurement, maintenance, management, support or oversight of such systems or equipment) | Databases<br><br>Biometric Identification Systems<br><br>Electronic Surveillance Systems |

| | Section | Description | Summary | Applicable Emerging Technology | Applicable Case Law | Case Law Findings |
|---|---|---|---|---|---|---|
| Protection of Freedoms Act (PoF) 2012 | 1-16 | Part 1: Regulation of Biometric Data | Provisions in respect of the retention and destruction of fingerprints, footwear impressions and DNA samples and profiles taken during a criminal investigation. | Databases<br><br>Biometric Identification systems | S and Marper v United Kingdom [2008] ECHR 1581(2) | The Act was brought in in response to the European Court of Human Right's 2008 judgment. In this case, the court ruled that the blanket retention of DNA profiles taken from innocent people posed a disproportionate interference with the right to private life, in violation of Article 8 of the European Convention on Human Rights. |
| | | | | | Gaughran v United Kingdom (45245/15) [2020] 2 WLUK 607 | the argument that "the more data is retained, the more crime is prevented" would in practice be tantamount to justifying the storage of information on the whole population and their deceased relatives, which would most definitely be excessive and irrelevant (para 89) |
| PoF: Part 1 | 1 | Destruction of fingerprints and DNA profiles | Material taken or held by the police must be retained on a statutory basis | Databases | | |

| | | | | |
|---|---|---|---|---|
| | | | provided by the PoF, or destroyed. Fingerprints and DNA profiles must be destroyed if taking of material was unlawful or was taken from individuals whose arrest was unlawful/ based on mistaken identity. | Biometric Identification systems |
| PoF: Part 1 | 3 | Persons arrested for or charged with a qualifying offence | Individuals arrested or charged with but not convicted of a qualifying offence: material retained for three years.<br><br>If person was previously convicted of | Databases<br><br>Biometric Identification systems |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | recordable offence or convicted before material needs to be destroyed by virtue of this section, the material is retained indefinitely. | | | |
| PoF: Part 1 | 4 | Persons arrested for or charged with a minor offence | Material destroyed after decision not to be charged or following acquittal | Databases<br><br>Biometric Identification systems | | |
| PoF: Part 1 | 5-6 | Persons convicted of a recordable offence; Persons convicted of an offence outside England and Wales | Material retained indefinitely. | Databases<br><br>Biometric Identification systems | Gaughran v United Kingdom (45245/15) [2020] 2 WLUK 607 | The authorities had decided on the indefinite retention of the photograph of an individual convicted of driving with excess alcohol, in addition to his DNA profile and fingerprints, the Court found a violation of Article 8. The authorities had failed to strike a fair balance between the competing public and private interests as there was no |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | | | reference to seriousness of offence and an absence of review. |
| | | | | | S & Marper v the United Kingdom | The retention for an unlimited duration of the photograph of an individual suspected of committing an offence who had not been found guilty carried a higher risk of stigmatisation than the retention of data on individuals who had been convicted of an offence (para 122). |
| PoF: Part 1 | 7 | Persons under 18 convicted of first minor offence | For custodial sentence for less than 5 years, material retained for 5 years, plus length of custodial sentence.<br><br>A custodial sentence longer than 5 years: material retained indefinitely. | Databases<br><br>Biometric Identification systems | | |

| | | | | |
|---|---|---|---|---|
| PoF: Part 1 | 8 | Persons given a penalty notice | Material may be retained for 2 years. | Databases<br><br>Biometric Identification systems |
| PoF: Part 1 | 9 | Material retained for purposes of national security | Retained if national security determination is in place. | Databases<br><br>Biometric Identification systems |
| PoF: Part 1 | 10, 11 | Material given voluntarily (10)<br><br>Material retained with consent (11) | S10 material is retained until it has fulfilled its purpose unless individual is convicted of recordable offence as data is retained indefinitely. | Databases<br><br>Biometric Identification systems |

| | | | | |
|---|---|---|---|---|
| | | | S11 individual's material may be retained for as long as person consents. | |
| PoF: Part 1 | 12 | Material obtained for one purpose and used for another | S12 in the event material was taken in connection with an investigation but leads to individual being charged/convicted for another offence, treat material as if it was taken in connection with latter investigation. | Databases<br><br>Biometric Identification systems |
| PoF: Part 1 | 13 | Destruction of copies | Any copy of fingerprints and DNA profiles are required to be destroyed. Copies of DNA may only be retained in a form which does | Databases<br><br>Biometric Identification systems |

| | | | | |
|---|---|---|---|---|
| | | | not allow individual to be identified. | |
| PoF: Part 1 | 14 | Destruction of samples | DNA samples is required to be destroyed once a DNA profile has been derived from it, or after six months. | Databases<br><br>Biometric Identification systems |
| PoF: Part 1 | 16 | Use of retained material | Limits the use of material retained under this Act to four conditions: national security; terrorist investigation; prevention or detection of crime/investigation of an offence/conduct of prosecution; or identification | Databases<br><br>Biometric Identification systems |

| | | | | |
|---|---|---|---|---|
| | | | of a deceased person/ | |
| PoF: Part 1 | 23 | Inclusion of DNA profiles on National DNA Database | DNA profiles must be recorded on the National DNA database. | Databases |
| PoF: Part 1 | 28 (2), (3) | Interpretation: Chapter 2 | “Biometric information” relates to a person’s physical or behaviour characteristics which can be used to verify the identity of the individual and is obtained/recorded with the intention that it be used for the purposes of a biometric recognition system. | Biometric Identification Systems<br><br>Electronic Surveillance Systems |

| | | | | |
|---|---|---|---|---|
| PoF: Part 1 | 28(3) | Interpretation: Chapter 2 | Biometric information includes skin patterns, physical characteristics, fingers/palms/iris/eye features, and voice or handwriting. | Biometric Identification Systems |
| PoF: Part 1 | 28(4) | Interpretation: Chapter 2 | “Biometric recognition system” is equipment operating automatically to obtain/record information about a person’s physical or behavioural characteristics. This information can then be compared with stored information for | Databases<br><br>Biometric Identification Systems<br><br>Electronic Surveillance Systems |

| | | | | |
|---|---|---|---|---|
| | | | the purposes of verifying identify | |
| PoF: Part 2 – Regulation of Surveillance | 29(1)(2) | Code of practice for surveillance camera systems | Preparation of a code of practice by the Secretary of State, which must contain guidance about surveillance camera systems. Guidance includes development or use of surveillance and the use or processing of images by virtue of such systems. | Electronic Surveillance Systems |
| PoF: Part 2 | 29(3) | Code of practice | Provisions may include considerations as to whether to use surveillance camera systems, types of system, | Electronic Surveillance Systems |

| | | | | |
|---|---|---|---|---|
| | | | technical standards for systems, locations, publications of information about systems, standards, access to/disclosure of information obtained, and complaints procedures. | |
| PoF: Part 2 | 29(6) | Code of practice | “Surveillance camera systems” mean CCTV or automatic number plate recognition systems; other systems for recording or viewing images for surveillance, systems for storing/receiving /transmitting/pro | Biometric Identification Systems<br><br>Electronic Surveillance Systems |

| | | | | |
|---|---|---|---|---|
| | | | cessing or checking images | |
| PoF: Part 2 | 34 | Commissioner in relation to code | Secretary of State must appoint Surveillance Camera Commissioner to ensure compliance, offer guidance, and review operation of the code. | Electronic Surveillance Systems |
| PoF | 37 | Judicial approval for obtaining or disclosing communications data | After a “relevant person” grants an authorisation to obtain communications data following a successful application, judicial approval is required. A “relevant person” is someone who holds office, | Databases |

| | | | | |
|---|---|---|---|---|
| | | | rank, or position in a local authority. Judicial authority must ensure that statutory tests and conditions have been met and that techniques are necessary and proportionate. | |
| PoF | 38 | Judicial approval for directed surveillance and covert human intelligence sources | Once a relevant person has granted an authorisation for the use of directed surveillance, judicial approval is required. The same procedural requirement as in S37. | Electronic Surveillance Systems |

| | Section | Description | Summary | Applicable Emerging Technology | Applicable Case Law | Case Law Findings |
|---|---|---|---|---|---|---|
| Regulation of Investigatory Powers (Sc) Act 2000 | 1 | Conduct to which the Act applies | This section describes and defines the conduct that can be authorised under this Part of the Act. Three types of activity are "directed surveillance", "intrusive surveillance" and the conduct and use of covert human intelligence sources. | Electronic Surveillance Systems | | |
| | 5 | Lawful Surveillance | Conduct is lawful if authorised in accordance with the Act and if carried out in | Electronic Surveillance Systems | | |

| | | | |
|---|---|---|---|
| | | accordance with that authorisation. | |
| 6 | Authorisation of directed surveillance | Conduct can only be authorised where it is necessary and proportionate. For it to be necessary it should be for the purpose of preventing or detecting crime or of preventing disorder; in the interests of public safety; or for the purpose of protecting public health | Electronic Surveillance Systems |
| 8 | Person entitled to grant authorisation of directed surveillance. | Individuals holding such offices, ranks or positions with relevant public authorities as are prescribed | Electronic Surveillance Systems |

| | | | |
|---|---|---|---|
| | | for the purposes of this subsection by order made by the Scottish Ministers. | |
| 10 | Authorisation of Intrusive surveillance | Conduct can only be authorised for the purpose of preventing or detecting serious crime; and if that the authorised surveillance is proportionate to what is sought to be achieved by carrying it out. Importantly, consideration should be given to whether the information which it is thought necessary to obtain by the | Electronic Surveillance Systems |

| | | | |
|---|---|---|---|
| | | authorised conduct could reasonably be obtained by other means. | |
| 11 | Rules for authorising intrusive surveillance. | An application should be made by a constable to the designated person. The designated person is set out in s10. | |
| 12 | Authorising intrusive surveillance urgent cases. | Mechanism for allowing Police Investigations and Review Commissioner staff to authorise conduct in urgent cases. | Electronic Surveillance Systems |
| 13 | Notification of authorisation of intrusive surveillance. | Notice to be given of grant or cancellation of authorisation of intrusive | Electronic Surveillance Systems |

| | | | | | |
|---|---|---|---|---|---|
| | | surveillance to a Judicial Commissioner. | | | |
| 14 | Approval required for authorisations to take effect | Authorisation of intrusive surveillance will not take effect until the grant of the authorisation has been approved by [ a Judicial Commissioner ] and written notice of the decision of that approval by that Commissioner has been given to the person who granted the authorisation. | Electronic Surveillance Systems | | |
| 19 | General rules about grant renewal and duration | Authorisation may be granted or renewed orally in any urgent case in which the | Electronic Surveillance Systems | HMA v Purves 2009 S.L.T. 969 | Held, that the online document, having been prepared personally by the superintendent, could be said to be a written document in terms of s 19, it bore the superintendent's name as |

entitlement to act of the person granting or renewing it is not confined to urgent cases; and in any other case, must be in writing.

authoriser and it was unreasonable to require a signature either pre or post printing when the 2000 Act imposed no such requirement and there was no case law to suggest such a formality (paras 11-12)

Opinion, (1) that the admissibility of the evidence, in the event that the surveillance was not authorised, did not fall to be determined where there was nothing in the evidence which suggested any infringement of the accused's art 8 rights (para 18); (2) that even if there had been a breach of an art 8 right, the evidence would not automatically become inadmissible as a hearing on the full circumstances in which the evidence was obtained would be required and regard would have to be had to the relative importance of the public interest as well as the

| | | | | |
|---|---|---|---|---|
| | | | | protection of the accused (para 19). |
| 20 | Cancellation of authorisation | Regulation of the circumstances of cancellation. | Electronic Surveillance Systems | |
| 24 | Issues and revision of codes of practice | Scottish Ministers should issue codes of practice that address the operation of this statute, part 5 of the Investigatory Powers Act 2016, and Part III of the Police Act 1997 relating to the regulation of interference with property or wireless telegraphy | Electronic Surveillance Systems | |
| 25 | Power to issue interim codes | Facilitates the issuing of interim codes until provisions | Electronic Surveillance Systems | |

| | | | | |
|---|---|---|---|---|
| | | | of s24 can be satisfied. | |
| | 26 | Effect of Codes of Practice | Codes of practice will not give rise to civil or criminal penalty where an individual fails to comply but may be taken into account in any related proceedings where relevant. | Electronic Surveillance Systems |
| Regulation of Investigatory Powers Act (RIPA) 2000 | 26 | Conduct to which Part II applies | This section describes and defines the conduct that can be authorised under this Part of the Act. Three types of activity are "directed surveillance", "intrusive surveillance" and the conduct | Electronic Surveillance Systems |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | and use of covert human intelligence sources. | | | |
| RIPA | 26(2) | Conduct to which Part II applies | "Directed surveillance" is defined as covert surveillance that is undertaken in relation to a specific investigation or operation which is likely to result in the obtaining of private information about a person (whether or not one specifically identified for the purposes of the investigation or operation); and otherwise than by way of an immediate response to | Electronic Surveillance Systems | Peck v. the United Kingdom<br><br>Perry v. the United Kingdom | The Court has drawn a distinction between the monitoring of an individual's acts in a public place for security purposes and the recording of those acts for other purposes, going beyond what the person could possibly have foreseen in order to establish the strict boundary of private life as secured under Article 8 in the sphere of secret surveillance measures and the interception of communications by the State authorities (Peck, paras 59-62; Perry, paras 41-42). |

| | | | | |
|---|---|---|---|---|
| | | | events or circumstances the nature of which is such that it would not be reasonably practicable for an authorisation under this Part to be sought for the carrying out of the surveillance. | |
| RIPA | 26(5) | Conduct to which Part II applies | Surveillance is not intrusive unless information is obtained which is of the same quality and detail that would be expected from a device on a residential premise or in a vehicle. | Electronic Surveillance Systems |

| | | | | | | |
|---|---|---|---|---|---|---|
| RIPA | 26(9) | Conduct to which Part II applies | Surveillance will be covert where it is carried out in a manner calculated to ensure that the person or persons subject to the surveillance are unaware that it is or may be taking place. | Electronic Surveillance Systems | Peck v. the United Kingdom<br><br>Perry v. the United Kingdom | Video recordings made in a public place using surveillance mechanisms may fall within Article 8 where their disclosure, by its manner or extent, goes beyond what the individuals could reasonably have expected. |
| RIPA | 26(10) | Conduct to which Part II applies | “Private information” is defined in relation to a person, includes any information relating to his private or family life. | Databases<br><br>Biometric Identification Systems<br><br>Electronic Surveillance Systems | | |
| RIPA | 27 | Lawful surveillance etc | All conduct defined in section 26 will be lawful, provided it is | Electronic Surveillance Systems | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | carried out in accordance with the authorisation to which it relates. Authorised conduct may cover any action taken either in the UK or abroad. | | | |
| RIPA | 28 | Authorisation of directed surveillance | Authorisations cannot be granted unless specific criteria are satisfied, namely, that the person granting the authorisation believes that:<br><br>the authorisation is necessary on specific grounds; and the authorised activity is proportionate to | Electronic Surveillance Systems | HMA v Purves 2009 S.L.T. 969 | Authorisation of directed surveillance was found lawful. |

| | | | | |
|---|---|---|---|---|
| | | | what is sought to be achieved by it. | |
| RIPA | 47 | Power to extend or modify authorisation provisions | The Secretary of State may, by order, change the types of activities which fall within the category of directed surveillance by providing that a type of directed surveillance will be treated as intrusive surveillance. Furthermore, he may, by order, provide those additional types of surveillance, which are not at present defined as directed or intrusive surveillance in section 26, will | Electronic Surveillance Systems |

| | | | | |
|---|---|---|---|---|
| | | | be covered by the Act and become capable of being authorised under Part II. | |
| RIPA | 48(2) | Interpretation of Part II | “Surveillance” includes— monitoring, observing, or listening to persons, their movements, their conversations or their other activities or communications ; recording anything monitored, observed, or listened to during surveillance; and surveillance by or with the assistance of a | Electronic Surveillance Systems |

| | | | | |
|---|---|---|---|---|
| | | | surveillance device. | |
| RIPA | 49 | Notices requiring disclosure | The power to enable properly authorised persons to serve notices on individuals or bodies requiring the disclosure of protected (e.g. encrypted) information which they lawfully hold, or are likely to, in an intelligible form. | Databases |
| RIPA | 49(1) | Notices requiring disclosure | Limits the information to which this power to serve notices applies. It does so by defining the various means by which the protected information in | |

| | | | |
|---|---|---|---|
| | | | question has been, or is likely to be, lawfully obtained. |
| RIPA | 49(2) | Notices requiring disclosure | Persons with the “appropriate permission” (see Schedule 2) may serve a notice imposing a disclosure requirement in respect of the protected information in question if there are reasonable grounds. |
| RIPA | 50 | Effect of notice imposing disclosure requirement | This section explains the effect of serving a notice imposing a disclosure requirement in various circumstances. |

| | | | | | | |
|---|---|---|---|---|---|---|
| RIPA | 51 | Cases in which key required | This section sets out the extra tests to be fulfilled if a key is required to be disclosed rather than the disclosure of protected information in an intelligible form. | | | |
| RIPA | 55 | General duties of specified authorities | This section describes the safeguards that must be in place for the protection of any material handed over in response to the serving of a notice under this Act. | Databases | | |
| | Section | Description | Summary | Applicable Emerging Technology | Applicable Case Law | Case Law Findings |

| | | | | |
|---|---|---|---|---|
| Investigatory Powers Act (IPA) 2016 | 2 | General duties in relation to privacy | A public authority exercising functions under the Act must have regard to whether the level of protection to be applied to information should be higher because of the sensitivity of that information. Must consider whether safeguards should be applied and taking the sensitivity of the information into account when considering whether obtaining the information is proportionate. | Databases<br><br>Biometric Identification Systems<br><br>Electronic Surveillance Systems |

| | | | | |
|---|---|---|---|---|
| | | | Subsection (5) includes examples of sensitive information, including items subject to legal privilege and information that identifies or confirms the identity of a source of journalistic information. | |
| IPA | 3 | Offence of unlawful interception | It is an offence to intentionally intercept a communication during its transmission without lawful authority. This applies to communications during transmission via a public telecommunicati | Electronic Surveillance Systems (interception technologies) |

| | | | | |
|---|---|---|---|---|
| | | | ons system, a private telecommunications system, or a public postal service. | |
| IPA | 4 | Definition of “interception” etc. | Subsections (1) to (5) outline what constitutes intercepting a communication during its transmission by a telecommunications system. Firstly, the person must perform a "relevant act", which is defined in subsection (2) and includes modifying or interfering with the system. Secondly, the consequence of the relevant act | Electronic Surveillance Systems (interception technologies) |

| | | | | |
|---|---|---|---|---|
| | | | must be to make the content of the communication available to a person who is not the sender or intended recipient. Thirdly, the content must be made available at a "relevant time", which means a time while the communication is being transmitted or any time when the communication is stored in or by the system. | |
| IPA | 6 | Definition of “lawful authority” | There are three conditions in which a person may have lawful authority to | Electronic Surveillance Systems (interception technologies) |

carry out interception. The first is through a targeted or bulk warrant. The second is through any of the other forms of lawful interception provided for in Ss.44 to 52 of the Act, such as interception in prisons or interception with consent. Thirdly, in relation to stored communications, interception is lawful if authorised by an equipment interference warrant or if it is in exercise of any statutory power for the

| | | | | |
|---|---|---|---|---|
| | | | purpose of obtaining information or taking possession of any document or other property or in accordance with a court order. | |
| IPA | 15(1) | Warrants that may be issued under this Chapter | There are three types of warrants which can be issued under this chapter: a targeted interception warrant, a targeted examination warrant and a mutual assistance warrant. | Electronic Surveillance Systems (interception technologies) |
| IPA | 15(2) | Warrants that may be | This section describes a targeted interception | Electronic Surveillance Systems |

| | | | | |
|---|---|---|---|---|
| | | issued under this Chapter | warrant and provides that such an interception warrant may authorise any activity for obtaining secondary data. | (interception technologies) |
| IPA | 15(3) | Warrants that may be issued under this Chapter | A targeted examination warrant grants the examination of material that has been collected under a bulk interception warrant. This warrant must be authorised whenever a member of an intelligence service needs to look at material which relates to a person who is known to be in | Electronic Surveillance Systems (interception technologies) |

| | | | | |
|---|---|---|---|---|
| | | | the British Islands and when he or she believes that it is necessary and proportionate to select the content of that person's communications for examination. | |
| IPA | 15(5) | Warrants that may be issued under this Chapter | This section explains that a warrant authorises any conduct necessary to fulfil what is authorised or required by the warrant, including the interception of communications not specifically described in the warrant, or the obtaining of | Electronic Surveillance Systems (interception technologies) |

| | | | | |
|---|---|---|---|---|
| | | | secondary data from such communications. | |
| IPA | 16 | Obtaining secondary data | Secondary data is systems data or identifying data attached to the communications being transmitted. Identifying data must be able to be separated so that it would not reveal the content of the communication. | Databases<br><br>Biometric Identification Systems<br><br>Electronic Surveillance Systems |
| IPA | 17 | Subject-matter of warrants | Subsection (1) sets out that a warrant may be directed towards a particular person or organisation, or a single set of premises. Subsection (2) | Electronic Surveillance Systems (interception technologies) |

| | | | | |
|---|---|---|---|---|
| | | | outlines that a warrant may also relate to a group of linked persons, or to more than one person or organisation, or set of premises in the context of a single investigation or operation. A warrant may also relate to testing or training activities, explained in more detail in subsection (3). | |
| IPA | 20 | Grounds on which warrants may be issued by the Secretary of State | The grounds include in the interests of national security, for the purpose of preventing or detecting | Electronic Surveillance Systems (interception technologies) |

| | | | | |
|---|---|---|---|---|
| | | | serious crime, in the interests of the economic well-being of the United Kingdom (in circumstances relevant to the interests of national security), or for giving effect to the provisions of a mutual assistance agreement. | |
| IPA | 31 | Requirements that must be met by warrants | Subsections (2) to (8) outline the information a warrant must contain. If a warrant relates to a single person, organisation/set of premises, the warrant must name that person/ | Electronic Surveillance Systems (interception technologies) |

organisation/those premises.

A warrant may relate to a group of persons linked by a common purpose or activity, or to more than one person/organisation/set of premises linked to a single operation/investigation. In such a case the link must be described and the warrant must name or describe as many of the persons, organisations or sets of premises as is reasonably practicable.

| | | | | |
|---|---|---|---|---|
| | | | The warrant must specify the factors that are to be used to identify the communications that are to be intercepted or selected for examination. | |
| IPA | 32 | Duration of warrants | An interception warrant will last for six months (unless it is cancelled earlier). If the warrant is not renewed it will cease to have effect after that period. Urgent warrants will last for five working days unless renewed. | Electronic Surveillance Systems (interception technologies) |
| IPA | 33 | Renewal of warrants | Subsections (1) to (3) state that a warrant may be renewed by | Electronic Surveillance Systems |

| | | | | |
|---|---|---|---|---|
| | | | the Secretary of State or a member of the Scottish Government. To be renewed, a warrant must be necessary and proportionate, applying the same tests as for issuing a warrant. As with an application for an interception warrant, the decision to renew the warrant must also be approved by a Judicial Commissioner. | (interception technologies) |
| IPA | 44 | Interception with the consent of the sender or recipient | Subsection (1) explains that communications may be intercepted if | Electronic Surveillance Systems (interception technologies) |

| | | | | |
|---|---|---|---|---|
| | | | both the person sending the communication and the intended recipient of the communication have given consent for the interception.<br><br>Subsection (2) states that the interception of a communication is authorised if either the sender or the intended recipient has consented, and surveillance has been authorised under Part 2 of RIPA. | |
| IPA | 53 | Safeguards relating to retention and | The issuing authority must ensure that arrangements are in place for | Databases<br><br>Electronic Surveillance |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | disclosure of material | securing those certain requirements are met relating to retention and disclosure of material obtained under the warrant. The number of persons who see the material, the extent of disclosure and the number of copies made of any material must be to the minimum necessary for the authorised purposes | Systems (interception technologies) | | |
| IPA | 61 | Power to grant authorisations | This section details the power for relevant public authorities to acquire | Databases<br><br>Electronic Surveillance Systems | Big Brother Watch v United Kingdom | RIPA 2000, Ch II for acquiring communications data from communication service providers violates art 8 as it is not in accordance with the law. Both |

| | | |
|---|---|---|
| communications data. Communications data is the ‘who,’ ‘when,’ ‘where’ and ‘how’ of a communication, but not its content. An authorisation can be granted where a designated senior officer in a relevant public authority is content that a request is necessary for one of the 10 purposes set out in subsection (7) and proportionate to what is sought to be achieved. Communications data cannot | (interception technologies) | these regimes were also held to violate art 10.<br><br>Note: the IPA replaced RIPA, which is why this case law has been put in this section. |

| | | | | |
|---|---|---|---|---|
| | | | be acquired for any other purposes and only certain authorities can use certain purposes, as outlined in Schedule 4. | |
| IPA | 61(5) | Power to grant authorisations | An authorisation may cover data that is not in existence at the time of the authorisation | Databases<br><br>Electronic Surveillance Systems (interception technologies) |
| IPA | 67 | Filtering arrangements for obtaining data | Outlines the power to establish filtering arrangements to facilitate the lawful, efficient, and effective obtaining of communications data by relevant public | Databases |

| | | | | |
|---|---|---|---|---|
| | | | authorities and to help determine whether the tests for granting an authorisation to obtain data have been met. The filtering arrangements will minimise the communications data obtained, thereby ensuring that privacy is properly protected. | |
| IPA | 99(2) | Warrants under this Part: general | A targeted equipment interference warrant authorises the interference with equipment for the purpose of obtaining communications | Electronic Surveillance Systems (interception technologies) |

| | | | | |
|---|---|---|---|---|
| | | | , information, or equipment data. | |
| IPA | 99(4) | Warrants under this Part: general | The acquisition of communications or other information through a targeted equipment interference can include monitoring, observing, or listening to communications or activities. As a result, it is not be necessary for such activity to be authorised separately under Part 2 of RIPA | Biometric Identification Systems<br><br>Electronic Surveillance Systems (interception technologies) |
| IPA | 100 | Meaning of “equipment data” | Under a targeted equipment interference warrant, | Biometric Identification Systems |

| | | | | |
|---|---|---|---|---|
| | | | equipment data means systems data or identifying data. To be equipment data, identifying data must be capable of being separated from the communication or item of information in such a way that, when separated, it would not reveal the meaning (if any) of the content of the communication or the meaning (if any) of an item of information. | Electronic Surveillance Systems (interception technologies) |
| IPA | 106 | Power to issue warrants to | Circumstances in which a law enforcement | Electronic Surveillance Systems |

| | | | | |
|---|---|---|---|---|
| | | law enforcement officers | chief can issue a targeted equipment interference warrant to an appropriate law enforcement officer, outlining the process and requirements. | (interception technologies) |
| IPA | 135(1) | Part 5: interpretation | “Communication” includes<br><br>anything comprising speech, music, sounds, visual images or data of any description, and signals serving either for the impartation of anything between persons, between a person and a thing or between things | Biometric Identification Systems<br><br>Electronic Surveillance Systems |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | or for the actuation or control of any apparatus. | | | |
| IPA | 135(2) | Part 5: interpretation | “Equipment” means equipment producing electromagnetic, acoustic, or other emissions or any device capable of being used in connection with such equipment. | Biometric Identification Systems<br><br>Electronic Surveillance Systems | | |
| IPA | 136 | Bulk interception warrants | A bulk interception warrant may be authorised to intercepted overseas-related communications or to obtain secondary data from such | Electronic Surveillance Systems (interception technologies) | Big Brother Watch v United Kingdom | The ECtHR held that the bulk interception regime under RIPA 2000, s 8(4) violates ECHR, art 8 due to lack of oversight.<br><br>A regime of bulk interception of communications did not contain sufficient “end-to-end” safeguards to provide adequate and effective guarantees against arbitrariness and the risk of abuse, even |

| | | | | | |
|---|---|---|---|---|---|
| | | | communications. | | though certain robust safeguards were identified (paras 424-427) |
| IPA | 137 | Obtaining secondary data | Outlines secondary data which can be obtained under a bulk interception warrant. | Electronic Surveillance Systems (interception technologies) | |
| IPA | 138 | Power to issue bulk interception warrants | The Secretary of State may issue a bulk interception warrant only if it is necessary and proportionate, for one or more specified statutory purposes. Subsection (1) makes clear that the interests of national security must always be one of those purposes. | Electronic Surveillance Systems (interception technologies) | |

| | | | | |
|---|---|---|---|---|
| IPA | 158 | Power to issue bulk acquisition warrants | A warrant may be authorised only where it is necessary and proportionate for one or more specified statutory purposes. The interests of national security must always be one of the reasons. The warrant must be approved by a Judicial Commissioner. A warrant may only be issued to the three intelligence agencies. | |
| IPA | 199(1) | Bulk personal datasets: interpretation | A bulk personal dataset is a set of information that includes personal data relating to | Databases |

| | | | | |
|---|---|---|---|---|
| | | | several individuals, the majority of whom are not, and are unlikely to become, of interest to the service in the exercise of its functions. | |
| IPA | 199(2) | Bulk personal datasets: interpretation | Defines personal data. The definition is the same as in the Data Protection Act 1998 (DPA), but this also includes data relating to deceased persons. | Databases |
| IPA | 200 | Requirement for authorisation by warrant: general | An intelligence service may not exercise a power to retain a BPD unless its retention is authorised by | Databases |

| | | | | |
|---|---|---|---|---|
| | | | either a “class BPD warrant” (authorising an intelligence service to retain, or retain and examine, any BPD of a class described in the warrant) or a “specific BPD warrant” (authorising an intelligence service to retain, or retain and examine, any BPD described in the warrant): | |
| IPA | 204 | Class BPD warrants | Authorises the retention and examination of datasets that can be said to fall into a class because they are of a similar type and raise similar | Databases |

| | | | | |
|---|---|---|---|---|
| | | | considerations. Subsection (2) specifies what an application for a class BPD warrant must include: a description of the class of bulk personal datasets and the operational purposes for which it is proposed to examine datasets of that class. | |
| IPA | 205(2) | Specific BPD warrants | The dataset does not fall within a class described by an existing class BPD warrant. An example of this could be a new type of dataset. | Databases |

| | | | | |
|---|---|---|---|---|
| IPA | 205(3) | Specific BPD warrants | A dataset falls within a class BPD warrant, but either S202 prevents the intelligence service from relying on a BPD class warrant or the service believes that it would be appropriate to seek a specific BPD warrant. | Databases |
| IPA | 205(6) | Specific BPD warrants | These outline the conditions, which are the same for class BPD warrants. The Secretary of State can issue a warrant if they believe that it is necessary for specified purposes and proportionate, | Databases |

and that adequate handling arrangements are in place. The Secretary of State must also consider that each operational purpose specified in the warrant is one for which the examination of the bulk personal dataset to which the application relates is or may be necessary, and that the examination of the dataset for such an operational purpose is necessary for the statutory purposes set

| | | | | |
|---|---|---|---|---|
| | | | out in subsection (5)(a). | |
| IPA | 221 | Safeguards relating to the examination of bulk personal datasets | The Secretary of State must ensure that arrangements are in force for securing that any selection for examination of data contained in BPDs is carried out only as far as is necessary for the operational purposes specified in the warrant (at the time of the selection); and the selection of any such data is necessary and proportionate in all the circumstances. | Databases |

| | | | | | | |
|---|---|---|---|---|---|---|
| IPA | Part 5;<br>Part 6;<br>Part 7 | Safeguards | These parts are all similar in that they outline the provisions for the duration, renewal, approval, modification, cancellation, implementation, and non-renewal of warrants. | Databases<br><br>Biometric Identification Systems<br><br>Electronic Surveillance Systems | | |
| | Section | Description | Summary | Applicable Emerging Technology | Applicable Case Law | Case Law Findings |
| Human Rights Act 1998 (HRA) | Schedule 1, Article 8 | Right to respect for private and family life | The right to respect his private and family life, his home, and his correspondence. There shall be no interference by a public | Databases<br><br>Biometric Identification Systems | Gaughran v United Kingdom (45245/15) [2020] 2 WLUK 607 | facial recognition can be applied to photographs. As a result, domestic courts must take account of this in examining the necessity of any interference with the right to respect for private life of an individual whose photograph has been taken by the authorities (paras 67-70). |

| | | | |
|---|---|---|---|
| authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety, or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others. | Electronic Surveillance Systems | R (on the application of Wood) v Commissioner of Police of the Metropolis [2009] EWA Civ 414 | Concerned the retention of photographs. It was acknowledged that such action could be an interference in terms of Article 8(1). That in this case it was clear they were in the pursuit of a legitimate aim but that it was not proportional. |
| | | Szabo and Vissy v. Hungary | A case concerning mass surveillance of communications, the Court acknowledged that it was a natural consequence of the forms taken by present-day terrorism that governments would resort to cutting-edge technologies, including the massive monitoring of communications, to pre-empt imminent attacks. In this case the Court held that the legislation allowing mass surveillance did not provide the necessary safeguards against abuse, because new technologies made it easy for the authorities to intercept large quantities of data relating even to people not in the category originally targeted by the |

| | | | | | |
|---|---|---|---|---|---|
| | | | | | operation. Moreover, measures of this kind could be ordered by the executive without any control and without any assessment as to whether they were strictly necessary, and in the absence of any effective judicial or other remedy. |
| HRA | Schedule 1, Article 9 | Freedom of thought, conscience, and religion | Everyone has the right to freedom of thought, conscience, and religion; this right includes freedom to change his religion or belief and freedom, either alone or in community with others and in public or private, to manifest his religion or belief, in worship, teaching, | Biometric Identification Systems<br><br>Electronic Surveillance Systems | |

| | | | | |
|---|---|---|---|---|
| | | | practice and observance. | |
| HRA | Schedule 1, Article 10 | Freedom of expression | Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. | Biometric Identification Systems<br><br>Electronic Surveillance Systems |
| HRA | Schedule 1, Article 14 | Prohibition of discrimination | The enjoyment of the rights and freedoms set forth in this Convention shall be secured without discrimination on any ground such as sex, race, colour, language, | Biometric Identification Systems<br><br>Electronic Surveillance Systems |

| | | | | |
|---|---|---|---|---|
| | | | religion, political or other opinion, national or social origin, association with a national minority, property, birth, or other status. | |
| Convention 108+ Convention for the protection of individual with regards to the processing of personal data | Article 2(a) | Definitions | “Personal data” means any information relating to an identified or identifiable individual (“data subject”) | Databases<br><br>Biometric Identification Systems<br><br>Electronic Surveillance Systems |
| Convention 108+ | Article 2(b) | Definitions | “Data processing” means any operation or set | Databases |

| | | | | |
|---|---|---|---|---|
| | | | of operations performed on personal data, such as the collection, storage, preservation, alteration, retrieval, disclosure, making available, erasure, or destruction of, or the carrying out of logical and/or arithmetical operations on such data | |
| Convention 108+ | 2(c) | Definitions | Where automated processing is not used, “data processing” means an operation or set of operations performed upon | Databases<br><br>Biometric Identification Systems |

| | | | | |
|---|---|---|---|---|
| | | | personal data within a structured set of such data which are accessible or retrievable according to specific criteria | Electronic Surveillance Systems |
| Convention 108+ | 3 | Scope | Each Party undertakes to apply this Convention to data processing subject to its jurisdiction in the public and private sectors, thereby securing every individual's right to protection of his or her personal data | Databases<br><br>Biometric Identification Systems<br><br>Electronic Surveillance Systems |
| Convention 108+ | 5(1) | Legitimacy of data processing and quality of data | Data processing must be proportionate, that is, appropriate in relation to the | Databases |

| | | | | |
|---|---|---|---|---|
| | | | legitimate purpose pursued and having regard to the interests, rights and freedoms of the data subject or the public interest. Such data processing should not lead to a disproportionate interference with these interests, rights, and freedoms. | Biometric Identification Systems<br><br>Electronic Surveillance Systems |
| Convention 108+ | 5(2) | Legitimacy of data processing and quality of data | Two other pre-requisites for a lawful processing are an individual's consent or a legitimate basis prescribed by law. | Databases<br><br>Biometric Identification Systems<br><br>Electronic Surveillance Systems |

| | | | | |
|---|---|---|---|---|
| Convention 108+ | 5(4) | Legitimacy of data processing and quality of data | Data processing is fair and transparent, does not go beyond the scope of the original purpose and that it is only preserved in a form that allows identification for the shorted possible period of time | Databases<br><br>Biometric Identification Systems<br><br>Electronic Surveillance Systems |
| Convention 108+ | 6 | Special categories of data | The processing of genetic data, personal data relating to offences, criminal proceedings and convictions, and related security measures, biometric data uniquely identifying a | Databases<br><br>Biometric Identification Systems<br><br>Electronic Surveillance Systems |

| | | | | |
|---|---|---|---|---|
| | | | person, personal data for the information they reveal relating to racial or ethnic origin, political opinions, trade-union membership, religious or other beliefs, health, or sexual life, shall only be allowed where appropriate safeguards are enshrined in law. | |
| Convention 108+ | 7 | Data security | The controller, and processor, takes appropriate security measures against risks such as | Databases |

| | | | | |
|---|---|---|---|---|
| | | | accidental or unauthorised access to, destruction, loss, use, modification, or disclosure of personal data. | |
| Convention 108+ | 8 | Transparency of processing | The controller must be transparent when processing data to ensure fair processing and to allow data subjects to understand and exercise their rights in the context of such data processing | Databases<br><br>Biometric Identification Systems<br><br>Electronic Surveillance Systems |
| Convention 108+ | 9 | Rights of the data subject | Lists the rights that every individual should be able to exercise concerning the processing of | Databases<br><br>Biometric Identification Systems |

| | | | | |
|---|---|---|---|---|
| | | | personal data. Each Party shall ensure, within its legal order, that all those rights are available for every data subject together with the necessary means to exercise them. | Electronic Surveillance Systems |
| Convention 108+ | 11 | Exceptions and restrictions | There can be an exception to this provision when it is necessary and proportionate for the prevention, investigation, and prosecution of criminal offences. | |

**Legislation**

**UK**

Criminal Procedure (Scotland) Act 1995
Data Protection Act 2018
Equality Act 2010
Human Rights Act 1998
Investigatory Powers Act 2016
Police and Fire Reform (Sc) Act 2012
Regulation of Investigatory Powers Act 2000
Regulation of Investigatory Powers (Sc) Act 2000
Police, Crime, Sentencing and Courts Act 2022
Protection of Freedom Act 2012
Scottish Biometric Commissioner Act 2020

**EU**

Trade and Cooperation Agreement between the European Union and the European Atomic Energy Community, of the one part, and the United Kingdom of Great Britain and Northern Ireland, of the other part [2021] OJ L149/10

**Preparatory Documents**

Proposal for a Regulation of the European Parliament and of the Council on European data governance (Data Governance Act) - Outcome of the European Parliament's first reading (Strasbourg, 4-7 April 2022), ST 7853 2022 INIT

## Appendix 6: Research Team

This review of emerging technologies in policing was undertaken between January and July 2022 by a team of researchers from the Department of Sociology, Social Policy and Criminology, the Department of Law, and the Department of Management, Work and Organisation, at the University of Stirling in Scotland. **The Principal Investigator was Dr Niall Hamilton-Smith.**

*Team Members*

**Dr Irena L. C. Connon, Department of Sociology, Social Policy and Criminology, University of Stirling**
Dr Irena Connon is a Research Fellow in the Department of Sociology, Social Policy and Criminology at the University of Stirling. She is a Social Anthropologist and transdisciplinary researcher whose research focuses on: 1) understanding cross-cultural experiences of environmental hazards and disasters, including oil spills, extreme weather, and industrial legacy contamination; 2) enhancing the inclusion of marginalised people in Disaster Risk Reduction developments; 3) risk communication, 4) climate-related displacement, and 5) developing transdisciplinary methodologies for applied-action research. She holds a PhD from the University of Aberdeen and has won national-level awards for excellence in knowledge exchange. Her research has been published in international peer-reviewed journals and has been used to inform national-level policy, including the current UK Government's response to weather-related emergencies. Since joining the University of Stirling in 2021, she has been working on several research projects that focus on children's climate change risk, the lived experience of flooding in Scotland, emerging technologies in policing, and supporting decision making for embedding the complexity and uncertainty associated with climate risk in policy. Prior to this, she held positions at the University of Dundee and at the University of Technology Sydney, Australia.
Email: irena.connon1@stir.ac.uk
Telephone: +44 (0)1786 467740

**Dr Mo Egan, Department of Law, University of Stirling**
Dr Mo Egan was admitted as a solicitor in 2007. Her doctoral research, funded by the Scottish Institute for Policing Research examined the policing of money laundering in a cross-jurisdictional context. In 2010 she was a founding member of the UACES Policing and European Studies Network which provided a forum of knowledge exchange for academic researchers, police practitioners and policy makers engaged in policing cross-border crime or crimes of cross-national concern. In 2019 she was appointed to the Scottish Graduate School of Arts and Humanities (SGSAH) Discipline + Catalyst for Law. She is a founding member of the Scottish Law and Innovation Network (SCOTLIN) and member of the Centre for Research into Information, Surveillance and Privacy (CRISP). In 2021 she joined the Review Board of the Journal of Legal Research Methodology and became a member of REPHRAIN (National Research Centre on Privacy, Harm Reduction and Adversarial Influence Online) Peer Review College. Dr Egan continues to research in the field of justice and home affairs with a particular interest in financial crime, inter-agency

cooperation in policing, privacy, and the interplay between state and non-state agencies in the delivery of justice.
Email: mo.egan@stir.ac.uk
Telephone: +44 (0)1786 467591

**Dr Niall Hamilton-Smith, Department of Sociology, Social Policy and Criminology, University of Stirling**
Dr Niall Hamilton-Smith is an Associate Professor of Criminology at the University of Stirling, an Associate Director of the Scottish Centre for Crime and Justice Research and a member of the Scottish Institute for Policing Research. Niall moved to Stirling in 2007, having previously been a researcher in government, primarily working on policing and crime reduction projects. In Stirling Niall has continued to work on a range of police-related research projects both directly for policing and for the Scottish Government. This has included innovative work on developing new techniques for mapping and assessing organised crime threats, a pilot for mapping community intelligence using a signal crimes framework, research around public disorder and hate crime, as well as work exploring the impact of camera technology in the policing of football crowds.
Email: niall.hamilton-smith@stir.ac.uk
Telephone: +44 (0)1786 466435

**Niamh MacKay, formerly of the Department of Law, University of Stirling**
Niamh Mackay was a Research Assistant at the University of Stirling. Her research interests focus on international human rights law. She holds a Masters in International Human Rights Law and Diplomacy from the University of Stirling and an MA in French from the University of Glasgow.

**Dr Diana Miranda, Department of Sociology, Social Policy and Criminology, University of Stirling**
Dr Diana Miranda is a Lecturer in Criminology at the University of Stirling. Her research aligns criminological and sociological approaches to understanding emerging biometric and data driven technologies in the Criminal Justice System. In particular, she explores how surveillance impacts our bodies and identities through processes of technologically mediated suspicion: in policing, criminal investigation, smart cities, security of borders and prisons. Before Stirling and SCCJR, Diana worked in various UK HE institutions (Northumbria University, Keele University, Open University and Birkbeck - University of London) and other European universities (Girona in Spain and University of Minho, University of Porto and University of Coimbra in Portugal). She has published widely on international journals such as Criminology & Criminal Justice, Policing & Society, Surveillance & Society, Information & Communications Technology Law and Information Polity.
Email: diana.miranda@stir.ac.uk
Telephone: + 44 (0)1786 467710

**Professor C. William R. Webster, Department of Management, Work and Organisation, University of Stirling**
William Webster is Professor of Public Policy and Management at the Stirling Management School, University of Stirling. He is a Director of CRISP (the Centre for Research into Information Surveillance and Privacy), a research centre dedicated to understanding the social impacts and consequences of technologically mediated

surveillance practices. Professor Webster has research expertise in the policy processes, regulation and governance of CCTV, surveillance in everyday life, privacy and surveillance ethics, as well as public policy relating to data protection, eGovernment, and electronic public services. He is currently co- Editor-in-Chief of the journal Information Polity, co-chair of the Scottish Privacy Forum and co-chair of the EGPA (European Group of Public Administration) Permanent Study Group on eGovernment, and between 2009 and 2014 he led the Living in Surveillance Societies (LiSS) COST Action. He has also led a number of international research projects, including the ESRC SmartGov (Smart Governance of Sustainable Cities) project and the European Commission funded Increasing Resilience in Surveillance Societies (IRISS) and 'ASSERT' projects.
Email: william.webster@stir.ac.uk
Telephone: + 44 (0)1786 467358




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: 978-1-80525-351-8 (web only)

Published by The Scottish Government, February 2023

Produced for The Scottish Government by APS Group Scotland, 21 Tennant Street, Edinburgh EH6 5NA
PPDAS1206982 (02/23)

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