SHRC
Scottish
Human Rights
Commission

Human Rights and New Technologies in Policing:

Issues Paper for the Independent Advisory Group on Emerging Technologies in Policing

May 2021

The Scottish Human Rights Commission was established by the Scottish Commission for Human Rights Act 2006, and formed in 2008. The Commission is the National Human Rights Institution for Scotland and is independent of the Scottish Government and Parliament in the exercise of its functions. The Commission has a general duty to promote human rights and a series of specific powers to protect human rights for everyone in Scotland.

www.scottishhumanrights.com

This Issues Paper has been produced by the Scottish Human Rights Commission as an independent analysis of the human rights issues engaged by new and emerging technologies in policing. It has been produced as a contribution to support the work of the Independent Advisory Group on Emerging Technologies in Policing, of which the Commission is a member.

The contents of this paper represent the views of the Commission as an independent National Human Rights Institution. They do not represent the views of the Independent Advisory Group as a whole.

Table of Contents

1. Introduction

1. New technologies play an increasingly critical role in our society, which presents both opportunities and challenges to the enjoyment of our human rights. From enhancing the realisation of civil and political rights such as freedom of expression and assembly, to supporting the delivery of certain economic and social rights - improving healthcare services and increasing the security of our communities, technology provides new ways for people to connect and communicate. However, the design, development and application of new digital technologies, which includes processing of personal data, by a range of actors presents significant challenges to human rights.[1]

2. States bear the primary duty to promote protect and fulfil human rights. They have a positive obligation to protect against discrimination and promote equality. We are in a crucial juncture in our digital age, which provides an opportunity to build on and prioritise the design, development and use of new digital technologies to advance human rights and equality. The use of new technologies[2] by Police Scotland and other law enforcement agencies raises important human rights risks and ethical questions. The Scottish Government needs to place human rights at the core of how new digital technologies are used in the criminal justice system. As recommended by the Council of

[1] For a further discussion on this see our submission to Scottish Government Consultation on the Digital Strategy for Scotland published in December 2020, available at SHRC website.

[2] New technologies include, but are not limited to: facial recognition software; biometrics, data analysis; robots (including drones); enhanced body-worn cameras; shotspotter; thermal imaging; smarter cruisers; automatic license plate recognition and artificial intelligence to analyse data. This term covers both AI and non-AI tech. The term new technologies and new digital technologies is used interchangeably in this paper.

Europe Convention for the Protection of Individuals related to Personal Data:

'the introduction and use of new technologies should take full account of, and not contravene, fundamental principles as the inherent dignity of the individual and the respect for the human body, the rights of the defence and the principle of proportionality in carrying out of criminal justice'.[3]

3. This paper provides an overview of the human rights standards that we recommend be taken into account by the Independent Advisory Group on Emerging Technologies in Policing ("the IAG"). As human rights are essential to all aspects of the policing and the development of new technologies, this paper covers the legal, science and innovation, and oversight workstream areas identified by the IAG. An exhaustive examination of all human rights engaged by the use of new technologies by the police is beyond the scope of this paper. The purpose of the paper is to inform and guide thinking on the IAG's work, in particular how the development, application and oversight of new technologies must align with human rights standards. It will be for the IAG and other advisory and regulatory bodies to ensure that they comply with their remit in this area.

4. The paper also highlights some of the challenges presented to the enjoyment of human rights by the use of new technologies. These challenges not only relate to core risks to the right to privacy and the prohibition of discrimination. Rather, depending on the purpose and context in which new technologies are employed, any human right can be breached – from the right to

[3] 1981 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data.

access to information and freedom of expression, to freedom of thought and of peaceful assembly and association.

5. This challenge is even greater as the design of new technologies is predominantly carried out by the private sector, where much of the technological expertise and financial investment lies. In this context, it is important to note that there is a legitimate expectation that private actors (e.g. the business enterprises which are both developing the technology and processing personal data) should comply with all applicable laws and respect human rights.[4] The Scottish Government has a duty to take appropriate steps to prevent, investigate, punish and provide redress for human rights abuses committed by private actors.

6. In order to minimise these risks, it is recommended that a human rights based approach is taken to the design, development and application of digital technologies, as exemplified by the PANEL principles.[5] It is important to ensure not only that current use of new technologies by both the state and business comply with existing human rights obligations, but that human rights are at the centre of their design and development through the adoption of a human rights based approach (HRBA).

[4] See second pillar of the UN General Principles on Business and Human Rights, available at https://www.ohchr.org/EN/ISSUES/BUSINESS/Pages/BusinessIndex.aspx#:~:text=%20United%20Nations%20Guiding%20Principles%20on%20Business%20and,in%20its%20resolution%2017%2F4%20of%2016%20June%202011.

[5] See section V of this paper for a HRBA.

2. Legal Framework: Human Rights Law

This section expands on the human rights framework and highlights the key human rights engaged by the use of new technologies.

7. As discussed in the introduction, even when new technologies have the potential to support the enjoyment of human rights, the way in which they are designed, developed, deployed, and the personal data collected from them, can present human rights risks. The impact and type of right affected is dependent on how they are designed; the purpose and context in which they are used; and the safeguards and oversight systems in place. It is therefore critical to identify the human rights legal framework under which the Police should use emerging technologies. It is also crucial that the State in meeting its due diligence obligations ensures the protection of human rights by third parties, including businesses.

8. There are clear human rights obligations that apply in this area derived from the Human Rights Act 1998, and international human rights law, together with non-discrimination duties that derive from the Equality Act 2010. It is concerning that a clear and explicit legal framework for the use of new technologies is missing in Scotland.[6] For example, there is an absence of legislation and clear policy guidance for the use of facial recognition technologies; unmanned aerial systems/vehicles (drone); or body cameras and the use of the personal data collected by these technologies.

[6] The Commission has raised this point several times before Government and Parliament, including in the use of the digital triage system by Police Scotland. see: https://archive2021.parliament.scot/S5_JusticeSubCommitteeOnPolicing/Inquiries/20190312SHRC-CyberKiosks.pdf

The Human Rights Act 1998 (HRA)

9. The HRA, which incorporates the European Convention on Human Rights into UK law, sets out the fundamental rights and freedoms that everyone in the UK is entitled to. The HRA has three main effects in practice:

   a) It requires all public bodies such as the police, local authorities and courts, and other bodies carrying out public functions, to respect and protect the human rights in the Convention, making them justiciable in British courts.

   b) It requires the courts, where possible, to interpret our laws in a way which is compatible with the Convention.[7]

   c) It requires that any new legislation passed by the Scottish Parliament is compatible with the rights set out in the Convention (via the Scotland Act 1998).

10. Section 6 of the Human Rights Act 1998 makes it unlawful for a public authority to act in a way which is incompatible with a Convention right (an 'act' also includes the failure to act). So, it is paramount that public authorities put in place an effective human rights framework when new technologies are used by law enforcement agencies. Articles 2 and 3 of the HRA in particular provide a minimum standard for the police when using their powers. This framework should also reflect ethical considerations, as covered in the remit of the IAG.

[7] See Section 2 and 3 of the HRA.

11. Other international standards that should be given due consideration are the jurisprudence and general comments of human rights bodies to which the UK is a member.[8] UN independent experts have also developed relevant guiding principles concerning the use of personal and non-personal information.[9] These principles will be referred to throughout this paper. The draft regulatory framework and code of ethics for AI solutions (Council of Europe)[10] and the Guiding Principles on Business and Human Rights should be also considered. The General Data Protection Regulation (GDPR) that came into force in the UK in May 2018 and the Equality Act 2010 are also relevant.[11]

Article 6 - Due Process and the Right to a Fair Trial

12. Article 6 of the European Convention of Human Rights guarantees that everyone charged with a criminal offence is entitled to certain protections, including the right to be presumed innocent until proven guilty, the right to a hearing with due guarantees and within a reasonable time, by a competent,

[8] For example, the UN Committee on social and economic rights has recommended in its General Comment No. 25 (2020) on Science that the development and use of technologies should be taken within a human rights framework, taking into account cross-cutting human rights principles such as transparency, non-discrimination, accountability and respect for human dignity. The UN Committee on the rights of the child has also made clear in its General Comment No. 25 (2021) on Digital Environment that the digital environment should be compliant with CRC - and that national legislation governing the digital environment should reflect this.

[9] See for example UN Special Rapporteur on Privacy Report on Artificial intelligence and privacy (2021) and/or UN Special Rapporteur on Freedom of Peaceful Assembly and Association Report on the exercise of the rights to freedom of peaceful assembly and association in the digital age (2019).

[10] The Draft Ethics Guidelines for Trustworthy AI were produced by the European Commission's High-Level Expert Group on Artificial Intelligence. The group is comprised of 52 representatives from academia, civil society and industry, and it was put together through an open selection process.

[11] These two pieces of legislation are beyond the scope of this analysis.

independent and impartial tribunal, and the right to have any conviction and sentence reviewed by a higher tribunal satisfying the same standards.

13. The police play a key role in the task of investigating allegations of criminal behaviour. This includes a number of activities beyond detention, such as interrogating suspects and witnesses, carrying out searches, undertaking surveillance (e.g. collecting facial images), and generally securing evidence (e.g. collecting DNA and fingerprints). As these aspects of police investigation practices take place within the context of a criminal process, they may have an important impact upon the fairness of a criminal trial under Article 6. These aspects include to both the presumption of innocence and evidentiary issues.

14. The respect for due process guarantees are fundamental in relation to the right of every person under the ECHR to be presumed innocent. Article 6 (2) is particularly important in this debate as it provides that 'everyone charged with a criminal offence shall be presumed innocent until proved guilty according to law'.[12] The obligation to respect the presumption of innocence not only applies to judges, but also to other public officials in general. The use of new technologies, for example in relation to biometric data retention of unconvicted persons, entrenches an interim categorisation of suspicion which adheres to individuals once they have come to be charged or arrested, thus distinguishes them from 'truly' innocent people who have not come to the attention of the police.

15. Article 6 is given a purposive interpretation that furthers the principle of fairness in the administration of justice. In terms of fair

12 See; Police facial recognition trial led to 'erroneous arrest'. The controversial trial of facial recognition equipment at Notting Hill Carnival resulted in roughly 35 false matches and an 'erroneous arrest', highlighting questions about police use of the technology. Sky news 7 Sept. 2017 available at http://news.sky.com/story/police-facial-recognition-trial-led-toerroneous-arrest-11013418.

rules of evidence it means the examination of the method in which the evidence was obtained[13] and admitted in the criminal proceedings.[14] Whether evidence is of dubious quality, the rights of the defence have been respected or it is improperly obtained can give rise to substantive unfairness which may render the criminal proceedings unfair.

Article 8 – Respect for Private and Family Life

16. A right to protection of an individual's private sphere against intrusion from others, especially from the State, was laid down for the first time in Article 12 of the United Nations Universal Declaration of Human Rights (UDHR) of 1948 (respect for private and family life). Article 8 of the ECHR and the Human Rights Act 1998 builds on this and requires respect for private and family life, home and correspondence. These concepts are sometimes indistinguishable and cover the protection of both the moral and physical integrity of the individual.

17. Article 8 therefore encompasses a wide range of issues and the use of new technologies has the potential to impinge on this right. Many technologies used by the police automatically collect data containing a significant amount of sensitive information about an individual's identity. While the police have been using fingerprints to identify people for over a century, now there is an ever-expanding array of biometric and behavioural characteristic data being collected and utilised that did not exist before. These include DNA, facial recognition, voice recognition, palm prints, wrist veins, iris recognition and gait analysis. Biometric information extracted from those tools contain large amounts of

[13] Barbera and others v Spain, 1988 (ECHR).

[14] Dombo BV v Netherlands, 1993 (ECHR).

personal and sensitive information such as unique genetic code and health data.[15]

18. In S and *Marper v the UK*, the European Court of Human Rights (EtCHR) expressed that:

"*the protection afforded by Article 8 of the Convention would be unacceptably weakened if the use of modern scientific techniques in the criminal justice system were allowed at any cost and without carefully balancing the potential benefits of the extensive use of such techniques against important private life interests*". [16]

19. Article 8 of the ECHR is a qualified right, which requires the State to justify any interference by reference to its legality, necessity and proportionality. This means that any restrictions should be:

- In accordance with the law "requires the impugned measure both to have some basis in domestic law and to be compatible with the rule of law, which is expressly mentioned in the preamble to the Convention and inherent in the object and purpose of Article 8. The law must thus be adequately accessible and foreseeable, that is, formulated with sufficient precision to enable the individual – if need be with appropriate advice – to regulate his conduct."[17]
- In pursuit of a legitimate aim: a public authority which intends to interfere with a person's rights under Article 8 must be able to demonstrate that such interference is based on one of the

[15] It is argued that facial recognition technology is becoming increasingly able to predict personal information, such as health conditions. See National DNA Database Ethics Group, Notes of the 38th meeting held on 7 June 2017 at Home Office, 2, Marsham Street, Westminster, London, SW1P 4DF

[16] S and Marper v the UK (Applications nos. 30562/04 and 30566/04).

[17] Ibid

legitimate aims set out in Article 8(2), including 'the prevention of disorder or crime' and 'the protection of the rights and freedoms of others'.

- Necessary in a democratic society: "An interference will be considered "necessary in a democratic society" for a legitimate aim if it answers a "pressing social need" and, in particular, if it is proportionate to the legitimate aim pursued and if the reasons adduced by the national authorities to justify it are relevant and sufficient[18] and sufficient procedural safeguards are available.[19]

20. There is a need for greater clarity about when the police or law enforcement agencies will both use new technologies and collect personal data. While there is a clear legal framework in relation to fingerprints, this is not the case for other biometric information and recognition systems used by the police.[20] While public safety and interest are paramount, a rights-based legal framework that respects Article 8 should be in place to guard against the risks of misuse and mishandling.

21. In relation to personal data management both the UK GDPR and the Committee of Ministers' Recommendation No. R (92)1 and R 87 (15)26 [21] advise that personal data kept for police purposes should be deleted if it is no longer necessary for the purposes for which it was stored. Personal data taken from individuals should

[18] See for example, Khan v the UK Application No 35394/97 (ECHR)

[19] In Klass v. Germany (Application no. 5029/71), for example, the European Court of Human Rights stated that it must be satisfied that any system of secret surveillance conducted by the State must be accompanied by adequate and effective guarantees against abuse.

[20] The use of databases and DNA retention has come into question in the United Kingdom. This include R (RMC and FJ) v MPS (Metropolitan Police Service). The High court held that the retention of the custody photographs amounted to an unlawful interference with R's and F's Article 8 rights – [2012] EWHC 1681 (Admin).

[21] Recommendation No. R 87 (15) to member states regulating the use of personal data in the police sector

be routinely deleted when it is no longer necessary to keep them for the purposes for which they were collected.[22]

22. Both international and national courts have found that the blanket retention of biometric data (DNA profiles (cellular samples and fingerprints and custody photographs) is unlawful and constitute an unjustified interference with the right to respect for private life, in violation of Article 8 of the ECHR.[23] The UN High Commissioner for Human Rights has noted that digital technologies '*threaten to create an intrusive digital environment in which both States and business enterprises are able to conduct surveillance, analyse, predict and even manipulate people's behaviour to an unprecedented degree*', and thus put the right to privacy at serious risk.[24]

Democratic Freedoms

23. Democratic freedoms are fundamental to the existence of a democratic society, where views and information can be exchanged. These freedoms include the right to respect for freedom of expression, peaceful assembly and association, and freedom of thought, conscience and religion (Articles 9 -11 of the ECHR).

24. While there is a general requirement to refrain from unjustified interferences, there may be situations where police are justified to do so. However, any interference with these rights must comply

---

[22] Article 40 of the CRC, for example, sets out children's rights in the criminal legal system.

[23] R (RMC and FJ) v MPS (Metropolitan Police Service) [2012] and R (on the application of S) v Chief Constable of South Yorkshire' and 'R (on the application of Marper) v Chief Constable of South Yorkshire' [2004] 1 WLR 2196, [2004] 4 All ER 193.

[24] Report of the Office of the United Nations High Commissioner for Human Rights to the Human Rights Council on 'The Right to Privacy in the Digital Age', 3 August 2018, A/HRC/39/29, p 1, available at https://undocs.org/A/HRC/39/29

with a number of conditions to be consistent with the Convention. These conditions are:

a) the interference must be in accordance with the law;
b) it must be in pursuance of a legitimate aim; and
c) it must be necessary in a democratic society.

25. Risks to democratic freedoms can arise from the widespread use of surveillance tools and AI-enabled technologies. The UN Special Rapporteur on the freedom of peaceful assembly and association has raised concerns about the increased use of digital surveillance tools in the context of peaceful assembly, noting that broad reasons such as national security or public order are routinely given to justify their use.[25] He argues that surveillance should in fact only be permitted on a targeted basis where reasonable suspicion can be demonstrated.

26. Furthermore, the proportionality principle requires that any surveillance measure used should be the least invasive option; mass surveillance, bulk data collection and facial recognition technologies employed at large events therefore raise proportionality concerns. The Special Rapporteur suggests that:

"In order to be permissible, targeted surveillance may occur only on the basis that such activities are adopted openly; are time-limited; operate in accordance with established international standards of legal prescription, legitimate aim, necessity and proportionality; and are subjected to continued independent supervision that includes robust mechanisms for prior authorization, operational oversight and review. Individuals and

[25] See Report of the UN Special Rapporteur (here) on the exercise of the rights to freedom of peaceful assembly and association in the digital age (2019)

groups should be notified if their rights are breached by surveillance, and effective remedies should be guaranteed."[26]

27. It has been widely documented around the world that the routine use of surveillance cameras during protests can have a chilling effect on those present and lead to disinclination to exercise the right to peaceful assembly due to concerns about privacy and how the data captured is used and stored.[27] Indiscriminate surveillance practices can thus have unintended and inhibiting effects on the exercise of our democratic freedoms.

28. The UN Special Rapporteur on freedom of opinion and expression has similarly raised concerns about the weak regulatory environment in which surveillance tools are deployed, arguing that '*interference with privacy through targeted surveillance is designed to repress the exercise of the right to freedom of expression'*.[28] The Special Rapporteur makes a number of recommendations for States, which includes but is not limited to, developing robust mechanisms for the approval and oversight of surveillance technologies and meaningful public

[26] Ibid.

[27] See for example: Report of the UN High Commissioner for Human Rights on 'Impact of New Technologies on the Promotion and Protection of Human Rights in the Context of Assemblies, Including Peaceful Protests', 24 June 2020, A/HRC/44/24, available at https://undocs.org/en/a/hrc/44/24 , and Asaf Lubin, '"We Only Spy on Foreigners": The Myth of a Universal Right to Privacy and the Practice of Foreign Mass Surveillance', Chicago Journal of International Law, 2018, 18, 502, available at https://chicagounbound.uchicago.edu/cjil/vol18/iss2/3/; and the Special Rapporteur on human rights in the context of counter-terrorism 'Report on Privacy' (2009), available at: untihttps://documents-ddsny.un.org/doc/UNDOC/GEN/G09/178/04/PDF/G0917804.pdf?OpenElement

[28] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, on 'Surveillance and Human Rights', A/HRC/41/35, 28 May 2019, available at: https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=24736

oversight and consultation in relation to the purchase of such technologies.[29]

Article 14 - Non–discrimination

29. The principles of equality and non-discrimination are central to human rights law and are recognised as norms in both the domestic and international framework. Article 14 of the ECHR enshrines the right not to be discriminated against in “the enjoyment of the rights and freedoms set out in the Convention”. Article 14 is not a standalone right, but operates in relation to discrimination on the enjoyment of the “rights and freedoms set forth in the Convention”. In other words, the guarantee provided by Article 14 has no independent existence. However, the ECtHR has recognised the applicability of Article 14 in cases where there had been no violation of the substantive right itself and has examined complaints under Article 14 in a variety of situations including in the criminal justice context.

30. While the use of new technologies to identify or profile potential suspects may, in principle, be a permissible means of investigation and can be an important law enforcement tool, it is important that enforcement agencies do not use broad profiles that reflect unexamined generalisations and/or stigmatisation. A recent report of the UN High Commissioner for Human Rights demonstrated the risks posed by the use of facial recognition technology to the right to peaceful assembly as well as its capacity to reinforce discrimination. The UN High Commissioner for Human Rights points to the error rate in facial recognition technologies, leading to individuals being wrongly flagged leading to detention and prosecution. Those who are particularly at risk of

[29] Ibid.

discrimination by this technology include 'Afrodescendants and other minorities, women or persons with disabilities.'[30]

31. Research on this area carried out by the EU Fundamental Rights Agency highlights how AI can amplify discrimination.[31] The UN Special Rapporteur on freedom of opinion and expression has found that, 'AI-driven newsfeeds may also perpetuate and reinforce discriminatory attitudes, while AI profiling and advertising systems have demonstrably facilitated discrimination along racial, religious and gender lines.[32] The European Union Network of Independent Experts on Fundamental Rights has expressed serious concerns about profiling on the basis of characteristics such as nationality, age or birthplace. These experts have recommended that profiling must strictly comply with the principles of necessity, proportionality and non-discrimination as well as be subject to close judicial scrutiny and should be periodically reviewed.[33]

32. Finally, discrimination can result not only from application but the design and development of digital technologies. As discussed further below, new digital technologies, particularly algorithms, are often dependent on data, which may be incomplete or contain bias. Such discrimination may then be reproduced and amplified

[30] Report of the UN High Commissioner for Human Rights on 'Impact of New Technologies on the Promotion and Protection of Human Rights in the Context of Assemblies, Including Peaceful Protests', 24 June 2020, A/HRC/44/24, available at https://undocs.org/en/a/hrc/44/24. See also https://www.disabilitynewsservice.com/international-human-rights-experts-to-meet-disabled-protesters-as-part-of-uk-probe/

[31] BigData: Discrimination data-supported decision making, FRA, 2018

[32] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, A/73/348, 29 August 2018, available at https://www.undocs.org/A/73/348 P 14 para 37.

[33] E/CN.4/2005/103, paras. 71–76

by their use by the police.[34] Additional obligations apply under the Equality legislation and the specific duties in Scotland.[35]

Article 2 – Right to Life

33. Article 2 safeguards the right to life and sets out the circumstances when deprivation of life may be justified. This is one of the most fundamental provisions in the Convention which imposes a duty to protect life through taking practical steps to address situations where there is an identifiable and real threat to life, including from attacks by other private individuals. The action required must be reasonable, without imposing an impossible or disproportionate burden on the authorities.

34. Article 2 is relevant to several aspects of State power, including policing, and provides a framework for the prevention and prosecution of homicide and the use of lethal force by the State through the mobilisation of its police and armed forces to combat terrorism, fight crime and control civil unrest.

35. The fundamental nature of Article 2 is also clear from the fact that it is "non-derogable": it may not be denied even in "time of war or other public emergency threatening the life of the nation", although a person's right to life is not breached if resulted from a lawful act as described in para. 2 of the Article (e.g. the police uses lethal force to stop a person carrying out unlawful violence).

---

[34] For example, in the UK, Foxglove and the UK Joint Council for the Welfare of Immigrants brought a lawsuit alleging that a 'streaming algorithm' which assigned risk according to nationality in the processing of visa applications 'entrenched racism and bias into the visa system', with 'a secret list of suspect nationalities automatically given a 'Red' traffic-light risk score' meaning that 'people of these nationalities were likely to be denied a visa'. They also argued that they 'discovered that the algorithm suffered from 'feedback loop' problems known to plague many such automated systems – where past bias and discrimination, fed into a computer program, reinforce future bias and discrimination'. Foxglove reported that the Home Office had settled the case, agreeing to disband the use of the algorithm.

[35] Further information on this can be found at https://www.equalityhumanrights.com/en/equality-act/equality-act-2010

Nonetheless, the force used must be absolutely necessary and strictly proportionate.

Article 3 - Prohibition of Inhuman, Degrading Treatment or Punishment

36. Article 3 of the Convention is an absolute right. This means that once it has been determined that certain treatment amounts to inhuman or degrading treatment, it can never be justified. The absolute prohibition of torture and inhuman or degrading treatment or punishment, operates differently to other rights (like Article 8 for example, which allows interferences with the right when it is justified). Article 3 of the ECHR has no limitations or exceptions for its interference.

37. Article 3 is relevant to several aspects of policing, including the use of force. For example, Police are permitted in some instances to use force to obtain biometric data (e.g. in the collection of fingerprints of foreign nationals)[36]. Use of force should be only used however when it is strictly necessary and proportionate to not violate Article 3. While new technologies could mean the introduction of less intrusive measures which are likely to reduce the risk of physical harm, there may be circumstances and contexts where their use could increase the likelihood of violence (e.g. during a tense public demonstration).

38. Actions that cause feelings of fear, anguish or inferiority capable of humiliating and debasing a person are also prohibited by Article 3 of the ECHR. In assessing whether conduct by the police attains a minimum level of severity to come within the scope of Article 3, attention must be paid to all surrounding circumstances.

[36] For example, under Eurodac Regulation (EU) No. 603/2013, all asylum seekers and migrants in an irregular situation apprehended in connection with an irregular border crossing – except for children under the age of 14 years – must provide their fingerprints

It is clear that the use of new technologies by Police Scotland must never amount to inhuman or degrading treatment or punishment.

Article 5 – The Right to Liberty and Security

39. Article 5 provides that everyone has the right to liberty and security of person. Paragraphs (1)(a) to (f) enumerate an exhaustive list of circumstances in which a person can be lawfully deprived of his liberty. Article 5 also lists the procedural safeguards to be met accompanying those permissible grounds on which a person can be deprived of his liberty. The underlying aim of Article 5 is to ensure that no one is arbitrarily deprived of his/her liberty

40. Police officers are given significant amounts of discretionary power to prevent and to investigate crime, which includes pre-trial detention and administrative detention and control orders. Many of these powers are highly intrusive, particularly the powers to detain a suspect and to search for evidence. As mentioned above, a plausible scenario that engages Article 5 of the European Convention of Human Rights is the deprivation of liberty to obtain fingerprints or other biometric data from an individual.

41. It also could be the case that deprivation of the liberty is prolonged due to the need of taking biometric information. It is therefore important to ensure that individuals, particularly vulnerable persons such as children, suspected victims of torture, sexual or gender-based violence are protected by this right and additional safeguards are met. Additional safeguard include: an appropriate adult being present when a vulnerable person is asked for their prints, access to a lawyer and a doctor and notification of their custody to a third party, humane conditions

therein as well as an strict limited duration of the depravation of liberty.[37]

42. The use of new technologies such as facial recognition, body worn cameras and drones to surveil people engaging in peaceful assembly and association would not only stifle legitimate freedoms, but potentially engage Article 5 if a person is unlawfully deprived of her liberty. It is imperative that any consideration to deprive a person of their liberty gives due consideration to the procedural and substantive guarantees articulated under Article 5.

3. Science and Innovation

43. Innovation has been fundamental for Digital technologies and has created a range of opportunities to enhance the availability, accessibility and quality of human rights such as the delivery of the right to the highest attainable standard of health and education. New technologies are used in innovative manners to help police to prevent crime.[38] In practice governments often rely on private contractors to design and develop new technologies in a public context. Private actors should comply with all applicable laws and respect human rights. The Scottish Government has a duty to take appropriate steps to prevent, investigate, punish and provide redress for human rights abuses committed by private actors.

44. This section considers some examples of new technologies used currently by the police by delineating the human rights concerns and the importance of independent oversight in the design of new technologies. The UN Secretary General has underscored, '[w]e

[37] See for example CRC standards including, best interests of the child, regards to the views of the child and evolving capacities core principles and CPT standards on detention

[38] See footnote no. 3

have a collective responsibility to give direction to these technologies so that we maximize benefits and curtail unintended consequences and malicious use'.[39]

45. Facial recognition software is a well-known example. The use of automated and live facial recognition in the UK is not new.[40] This technology matches facial images against existing databases to identify people. Both the accuracy and lawfulness of such tools have been questioned.[41] In addition, they may have an indirect effect on other human rights such as freedom of peaceful assembly.

46. Another example which has received media attention is predictive policing. This new technology is used, for example, in Kent and by some police forces in the US.[42] Predictive policing involves the use of statistical predictions to direct police resources. The concern with this is that algorithms and data analytics are kept secret (due to copyrights) and can in many cases reinforce existing biases in policing, as the data used to generate predictions is historic data. As a consequence, this may simply

---

[39] UN Secretary-General's 'Roadmap for Digital Cooperation: Implementation of the Recommendations of the High-level Panel on Digital Cooperation', A/74/821, 29 May 2020, Available at https://www.un.org/en/content/digital-cooperation-roadmap/

[40] See for example: The Metropolitan Police, 'Live Facial Recognition trial', available at https://www.met.police.uk/live-facial-recognition-trial/ and South Wales Police, Facial Recognition, available at <https://www.south-wales.police.uk/en/advice/facial-recognition-technology/

[41] HM Inspectorate of Constabulary in Scotland: Audit and Assurance Review of Facial Search functionality within the UK Police National Database (PND) by Police Scotland, January 2016. p7. And, Chris Foxx, 'Face recognition police tools 'staggeringly inaccurate'' (BBC, 15 May 2018), available at BBC website.

[42] PredPol, Kent Police Use PredPol to Prevent Violent Crime, 7 August 2013, available at <http://www.predpol.com/kent-police-use-predpol-toprevent-violent-crime/>; PredPol, LAPD Archives, available at <http://www.predpol.com/category/lapd/>; Timothy McLaughlin, 'As shootings soar, Chicago police use technology to predict crime' (Reuters, 5 August 2017), available at <https://www.reuters.com/article/us-chicago-policetechnology/as-shootings-soar-chicago-police-use-technology-to-predict-crime-idUSKBN1AL08P>

result in disproportionate police practices based on reinforce existing discrimination.

47. Algorithms have also been used to support risk assessments in bail and sentencing decisions.[43] Some courts are using algorithmic risk tools developed by private companies that calculate a risk score for individuals based on a list of factors, to inform their bail and sentencing decisions. Research on this has found that use of such tools may result in discrimination against certain category of individuals.[44] The other concern is emerging from corporate secrecy when using and developing the algorithms (the so called opacity), for example the algorithm used by Facebook and Google to detect violent extremism video and language is not known.

48. Despite noting the advances of new technologies the UN Special Rapporteur on freedom of opinion and expression called for immediate moratorium on the sale, transfer and use of surveillance tools in 2019 until '*robust human rights safeguards are in place to regulate such practice*'. The UN Special Rapporteur on freedom of opinion and expression has stated that surveillance tools can interfere with human rights, and yet they are not subject to any effective global or national control. He argued that, safeguards should include human rights due diligence, independent oversight, strict data protection laws and

[43] See Laurel Eckhouse et al., 'Layers of Bias: A Unified Approach for Understanding Problems with Risk Assessment' (2018) 20(10) Criminal Justice and Behavior.

[44] See Robert Weth, Risk and punishment: The recent history and uncertain future of actuarial, algorithmic, and "evidence-based" penal techniques, Sociology Compass, Volume 13, Issue 2, February 2019 at https://www.futurity.org/risk-assessment-tools-prison-2031222/ and Julia Angwin et al., 'Machine Bias', (Propublica, 23 May 2016), available at .t <https://www.propublica.org/article/machine-bias-risk-assessments-incriminal-sentencing>

full transparency of the use of surveillance technology as well meaningful consultation when buying these technologies.[45]

49. Participation in the regulation and governance of the design and development of digital technologies is therefore critical to create the conditions for innovation and to ensure that digital technologies are used to advance, rather than put at risk, equality and human rights. A HRBA[46] ensures that not only that current uses of new technologies comply with existing human rights obligations, but that human rights are placed at the centre of the design and development of these technologies.

4. Accountability and Oversight

50. Accountability is central to the protection of human rights. It requires both effective monitoring (oversight) and effective remedies. Effective accountability requires the duty bearers to provide for the development of adequate laws, policies, institutions, administrative procedures and redress mechanisms.

51. In this context, there are a number of crucial considerations when debating accountability related to the private sector:

a) The role of private actors in developing new technologies, including bias and quality assurance;
b) The adequate people participation in the development of new technologies. AI literacy is crucial to increase competence and better understanding of their implication for our lives.
c) Sharing of information across State agencies and private/commercial actors.

---

[45] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, on 'Surveillance and Human Rights', A/HRC/41/35, 28 May 2019, available at https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=24736

[46] See section V for human rights based approach to new technologies.

52. There has been increased regulation in this area which makes clear that (personal) data should not be shared across government departments and agencies unless specific in the law.[47] Data Protection legislation in the UK and throughout the wider EU provides a framework for the handling of personal data. In summary, personal data are data which relate to a living individual who can be identified from it directly or with other information which is in the possession of, or is likely to come into the possession of, the data controller (i.e. the organisation using the information). The Council of Europe Recommendation R(92)1 'on the use of the 24 analysis of DNA within the framework of criminal justice system' sets out that samples collected for DNA analysis and the information derived from such analysis for the purpose of the investigation and prosecution of criminal offences must not be used for other purposes. Linkage and sharing of personal data beyond criminal law purposes should be defined by law and subject to individuals' consent when appropriate.

53. Accessible, affordable, timely and effective remedies are a critical safeguard in the use of new technologies in the public (and private) sector. Individuals have a right to access justice and to an effective remedy under international human rights law, both in relation to State use of these technologies as well as private actors. The third pillar of the UN Guiding Principles on Business and Human Rights refers to three categories of grievance mechanisms through which individuals should be able to seek redress.[48] These are State-based-judicial and -non-judicial

---

[47] See Disability groups concerns with data sharing at: https://www.disabilitynewsservice.com/international-human-rights-experts-to-meet-disabled-protesters-as-part-of-uk-probe/

[48] UNGP Pillar 3, available at https://www.ohchr.org/documents/publications/guidingprinciplesbusinesshr_en.pdf

'Expert Meeting on the Technology Sector and Access to Remedy through Non-State-Based Grievance Mechanisms', Human Rights, Big Data and Technology Project and

mechanisms and non-State-based grievance mechanisms. While state based grievance mechanisms form the foundation of a system of remedies, non-State grievance mechanisms should complement such a wider system for impacts to be remediated quickly and directly by companies thereby also preventing future harms.[49] For example, the new Biometric Commissioner should review the existing policies in this area and define the required criteria in compliance with human rights. Complaint mechanisms play an important role in protecting against potential abuses and arbitrariness.

54. The protection of an open society requires also democratic accountability. The UN standards for oversight bodies clarify that is crucial to

> "(*E)stablish or maintain existing independent, effective, adequately resourced and impartial judicial, administrative and/or parliamentary domestic oversight mechanisms capable of ensuring transparency, as appropriate, and accountability for State surveillance of communications, their interception and the collection of personal data.*" [50]

55. Sufficient information regarding the development, application and governance new technologies should be in the public domain to maintain accountability and public confidence in their use.[51] Systems should also be subject to regular test and audits (due diligence process) to ensure both accountability and confidence. This should be accompanied by robust mechanisms for the

---

OHCHR, 11 June 2019, available at https://www.ohchr.org/Documents/Issues/Business/B-Tech/HRBDTOHCHRExpertMeetingTunis6September2019.pdf

[49] Ibid.

[50] See also 2016 UN Resolution on the Right to Privacy in the Digital Age.

[51] S and Marper v UK, para 99 (ECtHR)

approval and oversight of such technologies. In order to avoid discrimination and other human rights harms diversity hiring practices and wide consultation could help to avoid bias. Human rights training for officials involved in the procurement and those focus on research and development, use and review of machine learning systems is also crucial.

56. Human rights risks also arise depending on whether data are shared or sold and if inferences are drawn through them.[52] As it may be impossible to know how data is used once it has been shared or sold, the full impact on the right to privacy – as well as other human rights – may not be known and the harm may be difficult to quantify, particularly as it may continue in the future. As we do not have certainty of where our data is or whether it has been shared or sold, the full impact on the right to privacy (and other human rights) may not be known and the harm may be difficult to assess.

57. The UN Special Rapporteur on freedom of opinion and expression has expressed concern for the lack of independent oversight, strict data protection laws and full transparency of the use of surveillance technology.[53] Other accountability tools which help with the oversight processes are human rights impact assessments, which are critical to identify adverse impacts to human rights. These should be included in internal oversight

[52] See for example: Cambridge Analytica', Privacy International, available at https://privacyinternational.org/taxonomy/term/605; 'Cambridge Analytica Explained: Data and Elections', Privacy International, 13 April 2017, available at https://medium.com/privacy-international/cambridge-analytica-explained-data-and-elections-6d4e06549491 ; Green v SCL Group Ltd and others [2019] EWHC 954 (ch), [3], available at https://www.judiciary.uk/wp-content/uploads/2019/04/17.04.19-cambridge-judgment.pdf

[53] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, on 'Surveillance and Human Rights', A/HRC/41/35, 28 May 2019, available at https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=24736

processes within public sector and private sector bodies, as well as independent oversight bodies.

58. The right to remedy is also crucial. Persons who have been subject to unlawful infringement to their human rights (e.g. privacy by hacking a device) must have access to an effective remedy.

5. Human Rights Based Approach in New Technologies

59. There is a lack of legislation regulating the overall design, development and application of new digital technologies. Specific legislation requires government to ensure that both public bodies and business[54] meet their obligations to protect, promote and fulfil human rights. It is important also to ensure that science and innovation place human rights at the centre of the design and development of new digital technologies.

60. A HRBA sets out five principles to ensure human rights are adequately reflected in both application and design of new technologies. These are: Participation, Accountability, Non-Discrimination, Equality, Empowerment and Legality (PANEL). Legality, Accountability and Participation are discussed widely across this paper.

[54] Businesses have also an due diligence obligations under international law and set out in the UN Guiding Principles on Business and Human Rights to respect human rights.

Participation. Everyone has the right to participate in decisions which affect them. Participation must be active, free, and meaningful and give attention to issues of accessibility, including access to information in a form and a language which can be understood.
Accountability. This requires effective monitoring of human rights standards. For accountability to be effective there must be appropriate laws, policies, administrative procedures and mechanisms of redress in order to secure human rights.
Non-discrimination and equality. A human rights based approach means that all forms of discrimination must be prohibited, prevented and eliminated. It also requires the prioritisation of those in the most vulnerable situations who face the biggest barriers to realising their rights.
Empowerment. People should understand their rights, and be fully supported to participate in the development of policy and practices which affect their lives. People should be able to claim their rights where necessary.
Legality. The full range of legally protected human rights must be respected, protected and fulfilled. A human rights based approach requires the recognition of rights as legally enforceable entitlements, and is linked in to national and international human rights law.

61. An HRBA provides a consistent guidance and a common language to understand the harm and a baseline for the types of expected actions States and businesses should take to respect human rights. HRBA covers not only the HRA, but all of Scotland' existing obligations under human rights law as well as

businesses' responsibilities to respect human rights.[55] Human rights provides clear parameters as to what is and what is not permitted and the actions States and businesses have to take under existing international law when interfering with fundamental rights and freedoms. It also frames the design and development of these technologies.

62. In addition to PANEL, a key principle in relation to digital technologies is transparency - which is closely connected to the accountability principle. Where public sector bodies procure technologies from private actors, the nature of these procurement arrangements are not always made public, or subject to an accountability process. This raises further risks to human rights, particularly where the private sector actor is able to access and/or use data or test a particular technology through the public sector. There is no independent quality check process attached to these technologies at the moment. There is no explanation for its introduction and what it means for people and there is little transparency at the point of application/ deployment of the new technologies. Therefore transparency becomes crucial for both greater public trust and accountability.

[55] Businesses have also an due diligence obligations under international law and set out in the UN Guiding Principles on Business and Human Rights to respect human rights.

6. Summary

New technologies play an increasingly critical role in our society, which presents both opportunities and challenges to the enjoyment of our human rights. The design, development and application of new digital technologies, which includes processing of personal data, by a range of actors presents significant challenges to human rights. Therefore their use by Police Scotland raises important human rights risks and ethical questions. This challenge is even greater as the design and development of new technologies is predominantly carried out by the private sector, where much of the technological expertise and financial investment lies.

States bear the primary duty to promote protect and fulfil human rights. They have a positive obligation to protect against discrimination and promote equality. The Scottish Government needs to place human rights at the core of how new digital technologies are used in the criminal justice system.

This paper provides a human rights analysis of new technologies and offers examples of current risks and damages. The paper covers mainly legal framework, science & innovation and oversight, which are areas of identified by the IAG.

Science and Innovation

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

In practice, governments often rely on private contractors to design and develop new technologies in a public context. Private actors should comply with all applicable laws and respect human rights. We have a collective responsibility to give direction to these technologies so that we

maximize benefits and curtail unintended consequences and malicious use.

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

The regulation and governance of the design and development of new technologies is therefore critical to create the conditions for innovation and to ensure that these technologies, particularly AI are used to advance, rather than put at risk, equality and human rights

HRBA

A HRBA sets out five principles to ensure human rights are adequately reflected in both the design, deployment and management of new technologies. HRBA provides a consistent guidance and a common language to understand harms and expectations.

In addition to PANEL, a key principle in relation to digital technologies is transparency - which is closely connected to the accountability principle. There is little transparency at the point of deployment of the new technologies

Legal Framework

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

also crucial that the private sector meets its due diligence obligations to ensure protection of human rights. Human rights are in place to guard against the risks of misuse and mishandling as well as providing effective remedy.

It is concerning that a clear and explicit legal framework for the use of new technologies is missing in Scotland. For example, there is an absence of legislation and clear policy guidance for the use of facial recognition technologies; unmanned aerial systems/vehicles (drone); body cameras and the use of the personal data collected by these technologies.

Sharing data is also a concern. There have been report of disabled people who were allegedly photographed by English police forces at an Extinction Rebellion protest and their details passed to the DWP. Human rights standards prohibits collection of personal data to intimidate participants in a protest.

The police play a key role in the task of investigating allegations of criminal behaviour. This includes a number of activities such as carrying out searches, undertaking surveillance (e.g. collecting facial images), interrogating suspects and witnesses, and generally securing evidence (e.g. collecting DNA and fingerprints, so Articles 5, 6 and 8 of the ECHR are paramount.

National and international courts have found violation of human rights in the blanket retention of biometric data: DNA profiles (cellular samples and fingerprints and custody photographs) and bulk surveillance of public.

Risks to democratic freedoms, this are Articles 9 – 11 of the ECHR can arise from the widespread use of surveillance tools and AI-enabled technologies. There is an increased use of digital surveillance tools in the context of peaceful assembly and freedom of expression under the auspices of national security or public order. This type of interference with our democratic freedoms should only be permitted if it is lawful, proportionate and necessary on a targeted basis where reasonable suspicion can be demonstrated. The proportionality principle requires that any surveillance measure used should be the least invasive option

Indiscriminate surveillance practices, bulk data collection and facial recognition technologies employed at large events therefore raise human rights (proportionality) concerns. This was confirmed by the ECtHR in the Big Brother Watch v. the UK and Centrum för Rättvisa v. Sweden cases regarding bulk surveillance.

The principles of equality and non-discrimination are central to human rights law. As discussed discrimination can be reinforced by AI. It is important that enforcement agencies do not use broad profiles that reflect unexamined generalisations and/or stigmatisation. For example, the use of facial recognition technology poses a risk not only to the enjoyment of the right to peaceful assembly but also reinforces discrimination. Those who are particularly at risk of discrimination by this technology include ‘Afrodescendants and other minorities, women or persons with disabilities’.

Oversight and Accountability

Accountability is central to the protection of human rights. It requires both effective oversight and effective remedies. Individuals have a right to access justice and to an effective remedy under international human rights law, both in relation to State use of these technologies as well as private actors.

In this context, includes also private actors role in developing new technologies and sharing of information across State agencies and private/commercial actors. Human rights and data protection laws are clear that linkage and sharing of personal data beyond criminal law purposes should only be permitted if defined by law and subject to individuals’ consent when appropriate.

Accountability mechanisms include independent, effective, adequately resourced and impartial judicial, administrative and/or parliamentary domestic oversight bodies. This should be accompanied by robust mechanisms for the approval and oversight of such technologies. It is the case that research and development of machine learning systems is largely driven by the private sector. Regulatory and monitoring bodies should ensure the use of new technologies comply with human rights standards.

Other accountability tools which help with the oversight processes are human rights impact assessments, which are critical to identify adverse impacts to human rights. This should happened before public procurement process and deployment. In order to avoid discrimination and other human rights harms diversity hiring practices to inform design and development and wide consultation could help to avoid bias.

Human rights training for officials involved in the procurement and those focus on research and development, use and review of machine learning systems is crucial to close the knowledge gap.

Transparency is also key for accountability. Sufficient information regarding the development, deployment and governance new technologies should be in the public domain to increase (AI) literacy and understanding of its impact in our lives.

The UN Guiding Principles on Business and Human Rights refer to the importance of both remedy and prevention of future harms. Complaint mechanisms play an important role in protecting against potential abuses and arbitrariness. Accessible, affordable, timely and effective remedies are a critical safeguard in the use of new technologies by the public and private sector.

ENDS