Northern Ireland Policing Board


# HUMAN RIGHTS REVIEW OF PRIVACY AND POLICING

# CONTENTS

# FOREWORD

I am pleased to present this Human Rights Review of Privacy and Policing. The report is an ambitious piece of work and the first of its kind for policing in Northern Ireland and elsewhere. It attempts to highlight how important the right to privacy is and its continued significance as policing and surveillance technologies become more and more sophisticated.

The Human Rights Advisor and officials have done extensive research and consulted widely over the last six months, from engaging with different branches in the Police Service of Northern Ireland (PSNI) to non-governmental organisations (NGOs) and other public bodies. Topics covered in this report include access to databases; biometric collection, searching, and retention; artificial intelligence; surveillance; digital forensics; and data protection at PSNI.

Access to data and technology like facial recognition have the potential to support officers in solving crimes and other duties. These tools must be used in a responsible and trustworthy way to ensure public trust and confidence rather than constraining its potential.

The Human Rights Advisor has made six formal recommendations where it has been identified that action is necessary. The recommendations reflect the need for a wider public debate around privacy and policing with stakeholders. The Policing Board is committed to taking an active role in the governance of data ethics in policing to ensure privacy rights are protected.

This Report has been drafted in line with the Board's Human Rights Monitoring Framework, which was reviewed and updated in 2021 and sets out the areas under scrutiny by the Advisor over the three-year period.[1] I welcome the findings of the report and the recommendations made by the Human Rights Advisor. I will ensure that the Board and its Committee continue to scrutinise the work of the PSNI during this period so that the recommendations and lessons identified in this report are implemented to improve policing. In conclusion, I would like to thank our Human Rights Advisor, John Wadham, for his work in producing this Report.

**DEIRDRE TONER**
Policing Board Chair

1 https://www.nipolicingboard.org.uk/files/nipolicingboard/publications/human-rights-three-year-programme-of-work-2021-2024.pdf

# EXECUTIVE SUMMARY

This report is concerned with the PSNI's powers to investigate crime and protect the public where that impacts on the right to privacy of people of Northern Ireland. In particular, it concerns the PSNI's use of surveillance equipment; listening devices; informants (Covert Human Intelligence Sources); surveillance of social media and the websites that people visit; databases and the collection, retention, sharing and access to data about a person (including their fingerprints, DNA profiles and facial images); access to other UK databases; the increase in closed-circuit television (CCTV), cameras on drones and helicopters, automatic number plate recognition; extraction of information from digital devices; and facial recognition systems. It also reviews the systems in place for the police to access all this information. Finally, it attempts to consider the systems of governance, control and regulation and the protections and remedies that are in place to try to prevent abuse of this important right.

This report is also concerned with what appears to be an absence of significant consultation by the police, the Department of Justice, or the Northern Ireland Office on issues of privacy. The driver for new facial recognition systems, biometric data retention, CCTV and ANPR is the Home Office and the College of Policing, which are often adopted in Northern Ireland without any public consultation. Transparency in policing is difficult when techniques of targeted surveillance are concerned. Nevertheless, what techniques are actually used by PSNI in secret is often exaggerated and distorted. However, it is precisely these factors which continue to undermine confidence in PSNI, especially in some communities. A service which would wish the public to believe that it is solidly built on the basis of 'policing by consent' must continue to strive to become more transparent as these techniques have greater and greater impacts on privacy.

Police services across the UK have approached emerging data-driven technologies in policing such as facial recognition in different ways, from adopting them very quickly without public consultation to implementing a data ethics governance framework. Police Scotland are a positive example when it comes to governing emerging technologies in policing and PSNI are in the advantageous position of being able to learn from mistakes and experiences of other police forces.

Police Scotland have developed a data ethics framework which can be used across the policing system. The framework proposes new checks and governance tools embedded into the existing change process and will seek both internal and independent advice to ensure that the adoption of new technologies is proportionate, ethically justifiable and aligned with Police Scotland and the Scottish Police Authority's (SPA) commitment to policing by consent. The Data Ethics Framework has been endorsed by Police Scotland and will be considered by the SPA for use across the Policing System in the coming months.[2]

**Chapter 2** of this report considers criminal, intelligence, and other databases that PSNI have access to. The chapter also considers the Home Office's National Law Enforcement Data Service (NLEDS). The LEDS is a unified, common interface to a new database currently being developed by the Home Office.[3] The current biometric collections that are used by law enforcement and immigration agencies will be unified in a single database, the Home Office Biometrics Programme.

**Chapter 3** considers the collection, searching and retention of biometric data and its impacts on privacy rights. This involves biometrics taken on arrest, such as DNA and fingerprints, but also the use of live-time facial recognition technology. This chapter considers the legal landscape regarding biometrics and PSNI's approach to facial recognition technology.

**Chapter 4** gives a brief overview of Artificial Intelligence (AI) and policing. PSNI employ some tools that make use of artificial intelligence, such as a software tool used for online research purposes. PSNI clarified that AI technology would not be involved in decision making and that these technological advances are challenges that all law enforcement agencies are grappling with.

2 See Appendix 3, Oversight, scrutiny and review workstream report by the Independent advisory group on emerging technologies in policing, available at: https://www.gov.scot/binaries/content/documents/govscot/publications/independent-report/2023/02/oversight-scrutiny-review-workstream-report/documents/oversight-scrutiny-review-workstream-report/oversight-scrutiny-review-workstream-report/govscot%3Adocument/oversight-scrutiny-review-workstream-report.pdf

3 https://privacyinternational.org/campaigns/uk-law-enforcement-data-service-leds-new-police-mega-database

**Chapter 5** considers general public surveillance, in particular the use of public space CCTV and Automated Numberplate Recognition (ANPR), Body Worn Video, and the role of the Biometrics and Surveillance Camera Commissioner. Most CCTV cameras present throughout Northern Ireland and Great Britain are not operated by the police, but rather by the private sector and public authorities, such as councils and transport authorities, and PSNI rely on these CCTV networks when investigating crimes.

**Chapter 6** considers the use of targeted surveillance and privacy rights, such as telephone interception, directed surveillance, communications data, and undercover policing. The chapter further considers the role of the Investigatory Powers Tribunal and the role of the Investigatory Powers Commissioner.

**Chapter 7** is concerned with data extraction from digital devices. This new wealth of information is both a challenge and opportunity for policing and poses new challenges to the regulation of intrusive policing powers. The PSNI has a Cyber Support Unit (CSU) that provides forensic mobile phone extraction capability. This chapter considers PSNI guidance regarding taking a device from a witness, victim or suspect.

**Chapter 8** lays out how PSNI manage data protection and privacy in their organisation. Clear data protection principles and well-functioning data governance in an organisation are key to making sure that Article 8 rights are protected – in any organisation that holds sensitive data about people's lives, but especially police services. Only someone who needs to access certain data to discharge their duties should be allowed to access certain data, about witnesses or suspects for example.

**Acknowledgements**

We would like to thank the PSNI for providing the information for this report and for the openness of those officers and staff in discussing the issues with the Human Rights Advisor and Policing Board officials. In particular:

- Cyber Crime Centre
- Forensic Services
- Data Protection Officer
- ACC Chris Todd
- Operations Department
- Justice Department
- Intelligence Branch
- Information and Communications Services
- Specialist Operations Branch
- City Centre Policing Team

We would also like to thank the following NGOs and public bodies for their assistance with this report:

- Investigatory Powers Commissioner's Office
- Information Commissioners Office
- Ada Lovelace Institute
- Committee for the Administration of Justice
- Big Brother Watch
- Irish Equality and Human Rights Commission

# RECOMMENDATIONS

**Overall Recommendation:**

There should be an open and public debate about data driven technology in policing including developments in and use of Artificial Intelligence and Algorithms, Biometrics, Digital Forensics, Surveillance, and Investigatory Powers. PSNI should aim to become an organisation driven by effective and efficient use of data in an ethical way. The ethical use of data is about responsible and trustworthy use of data to ensure public trust and confidence rather than constraining its potential.

**To this end, it is recommended that:**

### RECOMMENDATION 1

PSNI and the Policing Board agree a Memorandum of Understanding (MoU) to ensure early visibility and oversight of any new strategy, policy or practice under consideration by PSNI. The MoU would cover all novel deployment, use of technologies and focus on human rights, privacy, ethical and equality considerations alongside any issues having an impact on public perception or confidence. This MoU should be in place by November 2023.

### RECOMMENDATION 2

The Policing Board and PSNI should hold a round-table in January 2024 with key external stakeholders to examine the developments in data-driven technology in policing, its value and the need for effective governance. Stakeholders might include the Minister of Justice, the Department of Justice, Information Commissioner's Office, the Police Ombudsman for Northern Ireland, the Northern Ireland Human Rights Commission, the Equality Commission for Northern Ireland, the Attorney General, local academics, human rights NGOs and key voluntary sector organisations.

**RECOMMENDATION 3**

Once a year, starting in November 2023 PSNI should present to the Performance Committee an update on developments in data driven technology including what systems have been implemented, what systems are being considered. This should include how those system assist PSNI with objectives, the human rights implications and any additional necessary governance arrangements.

**RECOMMENDATION 4**

By January 2024 the PSNI should develop a Data Ethics Governance Framework to ensure policing is driven by effective and efficient use of data in an ethical way.

**RECOMMENDATION 5**

By April 2024 PSNI should produce a Data Ethics Strategy engaging with external stakeholders and the wider public on the value of data driven technology, its development and use and how ethical and privacy safeguards will be effectively addressed.

**RECOMMENDATION 6**

The PSNI should give more immediate consideration to the following specific issues:

**a.** The PSNI should set out its current use and future proposals on facial recognition systems in a special report to the Policing Board. Any proposals should consider the protections that the Metropolitan Police and other police forces are likely to put in place. This should also include privacy, equality and human rights impact assessments and the PSNI's plans to consult the public on its proposals.

**b.** The Policing Board should invite the Biometric and Surveillance Camera Commissioner to visit Northern Ireland and to give evidence about his work generally and particularly his assessment of the PSNI and the issues more generally in Northern Ireland.

**c.** As there is currently no College of Policing guidance available around artificial intelligence systems the PSNI should develop both internal guidance and a public facing document that explains PSNI's approach to the technology.

**d.** The PSNI should consider using and adapting the Home Office's proposals for maintaining public trust[4] in CCTV systems by:

- Undertaking Data Protection Impact Assessments (DPIAs) prior to the use of a new biometric technology or a new application of an existing biometric technology, inviting scrutiny from an independent ethics panel, regulators and the Board
- As a matter of transparency, PSNI should publish all their Data Protection Impact Assessments and their Privacy Impact Assessments
- Follow all the relevant Codes including Surveillance Camera Code of Practice
- Consider the findings of the Home Office's Custody Image Review and ensure that the Commissioner's and ICO's guidance on the use of images is followed.

**e.** In view of the fundamental issues of ECHR compliance with the continued retention of biometric samples by the PSNI it is essential that the Assembly and the Department of Justice act on the appointment of a Biometric Commissioner for Northern Ireland. This would also be an opportunity to appoint an Investigatory Powers Commissioner for Northern Ireland.

**f.** Given the fact that there is almost no public information available on how to challenge the retention of DNA and other identity data held by the PSNI, the PSNI should consider how to increase public awareness of the procedures.

4 Biometrics Strategy: Better public services Maintaining public trust, Home Office, June 2018.

# CHAPTER 1:
# INTRODUCTION



1. In many common law countries including in the United Kingdom the right to privacy has been one of the weakest and least understood human rights. As recently as 1984 the courts accepted that there was very little privacy protection provided even for our conversations on the telephone (Malone v Commissioner of Police of the Metropolis). Until the year 2000, when the Human Rights Act came into force, the majority of covert surveillance procedures used by police and law enforcement officials were largely unregulated or, only regulated by obscure or secret sets of rules.

2. Perhaps the only part of the right to privacy that has any longer history is the right to privacy in the context of private property which can be traced back to Roman law, and in England to the Magna Carta in the 13th Century and the English Civil War.

3. Article 8 of the European Convention on Human Rights (ECHR) provides an explicit protection of the right to privacy:

   '1. Everyone has the right to respect for his private and family life, his home and his correspondence. 2. There shall be no interference by a public 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 wellbeing 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.'

4. Article 8 covers four areas, namely: private life, family life, home and correspondence. Some matters, of course, span more than one interest. The primary purpose of Article 8 is to protect against arbitrary interferences with private and family life, home, and correspondence by a public authority.[5]

5. This report is concerned with the PSNI's powers to investigate crime and protect the public where that impacts on the right to privacy of the people of Northern Ireland. In particular, it concerns the PSNI's: use of surveillance equipment, listening devices; informants (Covert Human Intelligence Sources); surveillance

5 *Libert v. France*, paras 40-42

of social media and the websites that people visit; databases and the collection, retention, sharing and access to data about a person (including their fingerprints, DNA profiles and facial images); access to other UK databases like store cards, employee records, bank accounts; the explosion of close circuit television, cameras on drones and helicopters, automatic number plate recognition, extraction of information from digital devices, and facial recognition systems. It also concerns the systems in place for the police to access all this information. Finally, it attempts to consider the systems of governance, control and the regulation and the protections and remedies that are in place to try to prevent abuse of this important right.

6. Human rights are not, however, designed to prevent police officers from doing their jobs. They provide positive duties on them to protect life and prevent ill-treatment. The PSNI would be failing in their duty if they did not explore and use technologies that might save lives or protect vulnerable people from imminent risks.

7. This report does not consider the issues involved in policing social media by the PSNI or the investigation of hate incidents, hate crime or other offences that may have resulted on Twitter, Facebook, etc.

8. Currently the PSNI can access databases with 18.5 million peoples' records[6], 58.5 million driver records, and 62.6 million vehicle records.[7] Additionally, Northern Ireland has several traffic cameras - 234 active sites, 109 of which are permanent.[8] There is also the possibility of live time access to seek matches with the 18.5 million facial images on the Police National Database (PND) in the UK linking to the Driver Vehicle Licensing Agency (DVLA), UK Border Agency, UK Visa and Immigration and the Ministry of Defence, which will become even more of a reality when the Home Office Biometrics Programme concludes.

9. Novel technologies, including connected vehicles and the Internet of Things (IoT) and other devices, have developed at pace over the past five years and rates of adoption will almost certainly increase. All new models of car sold in the European Union now have embedded SIM cards to contact emergency services when required. In 2016, 4.6 billion IoT devices were connected worldwide, compared to 19.8 billion in 2023.[9] Data related to connected vehicles, smart homes, and

6 Office of the Biometrics and Surveillance Camera Commissioner, Annual Report 2021/22, para 139
7 Alexander Babuta, Big Data and Policing, Royal United Services Institute, https://static.rusi.org/201709_rusi_big_data_and_policing_babuta_web.pdf. Note that these figures are from 2017.
8 https://www.nidirect.gov.uk/articles/types-and-locations-safety-cameras
9 https://www.statista.com/statistics/1101442/iot-number-of-connected-devices-worldwide/

connected cities offers additional opportunities for public authorities to achieve positive operational outcomes. Successful prosecutions have incorporated smart watch, smart speaker, vehicle, and video doorbell data.[10]

10. Technology and data systems are developing and changing all the time and, where possible, this report picks up developments that PSNI is or is about to be part of. Artificial Intelligence (AI) systems, which are likely to become more and more prevalent, can only be touched on in this report when they interact with the other systems that are set out above. Some of the methods of surveillance are secret or sensitive but this report is designed to provide a degree of transparency over these powers and procedures and is based on the idea that 'sunlight is the best disinfectant'.[11]

11. This is the first attempt to assess privacy and policing in Northern Ireland by the Policing Board. NGOs and other organisations have, however, scrutinised police forces in England and Wales in relation to privacy and have challenged law enforcement agencies in the courts, specialist tribunals and in the European Court of Human Rights (ECtHR). More recently the use of 'live time' facial recognition technology (not yet adopted by the PSNI) has already been subject to a number of challenges. This seems to be an area which receives relatively little attention from civic society and human rights NGOs despite their active role in many other issues around policing.

12. It is hoped that this report will provide some guidance to those that read it on what the PSNI is actually doing – police surveillance can often be an emotive and exciting topic but this often results in people either overestimating the extent of being 'spied on' all the time or alternatively assuming that all police surveillance is minimal and justified. Not surprisingly the actual position is more complex and, unfortunately, the absence of our democratic leaders watching the watchers may lead to a 'surveillance state' creeping up on us. It's important to ensure openness and transparency save where there is a genuine and compelling reason not to be transparent, and that the line between the two is drawn in the right place.

13. Technological advancements do not necessarily herald only doom and gloom: AI has the potential to vastly improve policing's ability to prevent crime, manage its resources more efficiently and coordinate fast-moving responses to major incidents. Crime prevention and criminal investigation teams could use AI to speed

10 Home Office, Report on the Operation of the Investigatory Powers Act 2016, February 2023, p 23, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1134783/E02825581_Investigatory_Powers_Act_2016_ELAY.pdf

11 Louise Brandeis, Justice of the United State Supreme Court

up the identification of criminals and their motives; neighbourhood policing teams could benefit from a better understanding of community dynamics; major incident commanders could use AI systems to improve situational awareness and better visualise potential strategies and tactics; and police call centres could use AI systems such as those pioneered by Amazon and UPS to more efficiently route responses to calls for service.[12]

14. In addition to the Human Rights Act and ECHR Article 8[13], the collection, retention, and use of information about people is regulated by the Data Protection Act 2018, the Council of Europe's Data Protection Convention[14] and, for some retained purposes, the EU Data Protection Directive. Some of the rules discussed in this report are about to be subject to change, as there are Bills going through the Westminster Parliament that will alter the privacy landscape in the UK (Data Protection and Digital Information Bill).[15] Policing in the UK (including Northern Ireland) will also be subject to other changes because of the introduction of the National Law Enforcement Data Service (NLEDS), which is discussed in Chapter 3.

## DEMOCRATIC DEFICIT

15. Apart from the lack of information available to people in Northern Ireland about the activities of the PSNI in relation to our privacy there appears to be an absence of significant consultation by the police, the Department of Justice, or the Northern Ireland Office on these issues. The driving force for all these developments and some significant erosion of privacy appears to originate from the law enforcement agencies in the UK. The Home Office, the College of Policing and others are developing more and more techniques and sometimes there appears to be no equivalent democratic input in Northern Ireland, even during the times that the Assembly is functioning.

16. PSNI have not engaged in some of the more intrusive practices favoured by some other police services, but this report highlights the need for continued scrutiny and debate. There has been little public debate or discussion around facial recognition or other biometric surveillance techniques in Northern Ireland.

12 College of Policing (2020) Our Policing in England and Wales: Future Operating Environment 2040, accessed at: https://assets.college.police.uk/s3fs-public/2020-08/Future-Operating-Environment-2040-Part1-Trends.pdf
13 Guide to the Caselaw of the European Court of Human Rights, Data Protection, August 2022 and Practical Guide on the use of personal data in the police sector, Council of Europe, 15 February 2018.
14 https://www.coe.int/en/web/data-protection/convention108-and-protocol
15 https://bills.parliament.uk/bills/3322

17. The Biometrics and Surveillance Camera Commissioner summarised the issue very well:

'As a society, we are becoming inured to biometric surveillance, while technological developments have meant that our capability to prepare for, respond to and recover from global crises has increased beyond anything our forebears might have realistically imagined. When extended into other areas such as schools and impacting upon young people's lives, the sensitivities, and risks of what has been termed omniveillance are amplified. We must be able to have confidence in the whole ecosystem of surveillance, to be sure that what is technologically possible is only being done in a way that is both legally permissible and societally acceptable.'[16]

## THE NEED FOR FURTHER REGULATION

18. Some of the technological advancements mentioned in this report are currently being used by police services across the UK without a corresponding legal framework. To get the most from biometric surveillance technology, there will need to be a systemic approach to regulation along with clear standards for everything and everyone involved. Biometric capability in its widest sense could revolutionise the investigation and prevention of crime and the prosecution of offenders.

19. In 2021, the Justice and Home Affairs Committee launched an inquiry into the use of new technologies in law enforcement. The Committee seeks to explore the use of advanced algorithmic tools in activities to discover, deter, rehabilitate, or punish people who breach the law in England and Wales.[17] The findings of the inquiry are also relevant to policing in Northern Ireland. In their report 'Technology rules? The advent of new technologies in the justice system', the Committee highlights how the area of technology and law enforcement is still poorly understood and guidance is needed on how to apply existing legal frameworks to these new technologies:

The National Police Chiefs' Council are establishing a national Digital and Data Ethics Guidance group to "provide national support, particularly on complex cases." As it stands, however, there is no one place where guidance on the use of new technologies can be found, and, as far as we are aware, no clear requirement

16 Commissioner for the Retention and Use of Biometric Material Annual Report January 2021 – March 2022 And Surveillance Camera Commissioner Annual Report March 2021 – March 2022 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1135384/Biometrics__Surveillance_Camera_Commissioner_Annual_Report_21-22.pdf

17 Justice and Home Affairs Committee, New Technologies and the application of the law, accessed at: https://committees.parliament.uk/work/1272/new-technologies-and-the-application-of-the-law/

on Police bodies to produce it. Guidance, both general and specific, is urgently needed. The Government should require that national guidance for the use of advanced technological tools in policing and criminal justice is drawn up and, as part of their response to this report, should outline concrete plans for this. There is a need for a 'one-stop shop' collating all relevant legislation, regulation and guidance and drawing together high-level principles with practical user guides. This collation should be updated by the College of Policing on an ongoing basis, and direct users to the guidance and regulation relevant to their circumstance and need.'[18]

20. While public bodies, including the police, are required to disclose how data is processed, there is no obligation to disclose what type of technology is used to process this data:

'There are no systematic obligations on individual departments, public bodies, and police forces to disclose information on their use of advanced technological solutions. It is impossible for Parliament, press, academia, those responsible for procurement and—importantly—those subject to their use to scrutinise and challenge the use of technological solutions as they cannot know who is using what, for how long, for what purpose, or with what safeguards. This risks undermining trust in the police, the justice system, and the rule of law.'[19]

18 House of Lords Justice and Home Affairs Committee 1st Report of Session 2021–22 HL Paper 180 Technology rules? The advent of new technologies in the justice system, paras 73 to 75, accessed at https://committees.parliament.uk/publications/9453/documents/163029/default/

19 Ibid para 98.

# CHAPTER 2:
# CRIMINAL, INTELLIGENCE AND OTHER DATABASES

21. To provide an overview of the types of information police services collect, this chapter considers the different types of databases PSNI and other police services in the UK have access to and contribute to, the sharing arrangements and future developments.

## CRIMINAL DATABASES

22. **Police National Computer**

'The Police Service of Northern Ireland (PSNI) holds a broad range of criminality information including convictions, diversions and other penalties, procedural records such as arrests and acquittals and 'intelligence' information. We will access information held on the Police National Computer (PNC) and will have locally held police information on our systems. All of these sources make up an individual's criminal history information held by the PSNI.'[20]

23. The Police National Computer (PNC) is a system that stores and shares criminal records information across the UK. Law enforcement agencies use it to access information that will support national, regional and local investigations. The PNC holds all records of arrests and summons, regardless of the outcome, and is kept for a hundred years from the date they were born, regardless of the date of their death.

Other agencies, such as the Driver and Vehicle Licensing Agency (DVLA), also have restricted access to the PNC.[21] PNC also holds records of people who are or who are wanted for arrest, a person of interest (in relation to a criminal investigation) and missing persons. It also holds information on property (stolen vehicles and other stolen goods).

24. **Fingerprint and DNA Databases**

All Biometrics recovered by the PSNI from suspects in the course of an investigation are stored and speculatively searched on the following databases:

20 https://www.psni.police.uk/enacting-other-rights-under-data-protection-legislation
21 https://unlock.org.uk/advice/organisations-access-police-national-computer-pnc/

- **Fingerprints**
- National IDENT1 Fingerprint system;
- Paper sets held locally in the PSNI Fingerprint Bureau; and
- National Counter Terrorist Fingerprint Database (NCT FPDB).
- **DNA**
- Local Northern Ireland DNA Database (NIDNADB)[22];
- National DNA Database (NDNADB);
- National Counter Terrorist DNA Database (NCT DNADB)[23].

25. **Causeway**

There are a broad range of criminal justice organisations in Northern Ireland, including the PSNI, that hold and share information for legitimate and lawful purposes in relation to an individual's 'criminal history'. Since 2002, PSNI have joined several criminal justice organisations including Forensic Science Northern Ireland, the Public Prosecution Service, the Northern Ireland Courts and Tribunal Service, the Northern Ireland Prison Service and the Probation Board for Northern Ireland to implement a jointly owned system known as Causeway. Causeway is not a database, but a messaging system between the individual criminal justice organisations.

> 'The Police Service of Northern Ireland processes a large range of data for policing purposes including details of convictions, diversions and other penalties, investigative information including records such as arrests, intelligence information as well as biometric data. Once a person has been charged or reported for an offence, the Causeway system tracks the case through the Criminal Justice process and facilitates access to an individual's criminal history, including information uploaded to the Causeway system by us.'[24]

26. Where an individual is or has been investigated for one or more 'Recordable offences' (as defined by the Police and Criminal Evidence (Northern Ireland) Order 1989) the PSNI will upload this information to the PNC. This is accessible by all UK police services, law enforcement agencies and other registered bodies across the United Kingdom for policing and other regulated processes.

22 This is a local DNA database with records that cannot be added to the national database because the quality threshold of those specific records is too low for inclusion (the Scottish Police has a similar local database).

23 PSNI Interim Service Instruction Biometric Retention, https://www.psni.police.uk/sites/default/files/2022-09/Biometric%20Retention%20and%20Disposal%2016%20September%202022.pdf

24 https://www.psni.police.uk/about-us/our-policies-and-procedures/corporate-policy/service-instructions

To discharge its statutory obligations, the PSNI retains individual criminal history information for 100 years from the person's date of birth.

### 27. ACRO Criminal Records Office

ACRO (Association of Chief Police Officers Criminal Records Office) is the national police unit responsible for exchanging criminal conviction information between the UK and other countries. ACRO manages the Criminal Record Information System (UK-CRIS) with EU Member States. ACRO, which is part of the UK police service, employs more than 300 people, is based in Hampshire Constabulary and, as a result, enjoys policing powers. It was founded in 2006 following a decision by the then Association of Chief Police Officers (now NPCC):[25]

ACRO's board is independent of ACRO and chaired by the chair of the NPCC comprises of representatives from Government, policing and expert members and representatives from Northern Ireland.

### 28. Criminal record checks and disclosure

AccessNI was established in 2008 to deal with requests by employers and others for criminal history pre-employment checks.[26] This includes information held by the PSNI.[27] Lower-level cautions, fines, convictions will not appear in most checks but some more serious convictions and those involving vulnerable victims will usually appear. There are different levels of checks available, including 'Enhanced' checks but there are also systems of redress for those who believe that the record disclosed is incorrect.

Part V of the Police Act 1997 requires AccessNI, on receipt of an application for an 'Enhanced' criminal records check, to ask the PSNI whether any information is held which "might be relevant" for the job in question and "ought to be" included in the certificate.'[28]

25 It states: 'We do this by: Being global leaders in the provision of criminal records and bio-metric information to enable safeguarding and offender management; Coordinating a centralised and cost effective national resource that supports the fight against crime and minimises the financial burden on police forces; Working with international law enforcement partners to further enhance our criminal record exchange capability; Delivering continual improvement in our expert service to partners, customers and the wider public; and; Creating a culture of inclusion, development and progression for our staff https://www.acro.police.uk/s/#section-about-us

26 https://www.nidirect.gov.uk/campaigns/accessni-criminal-record-checks

27 https://www.psni.police.uk/enacting-other-rights-under-data-protection-legislation

28 https://www.psni.police.uk/enacting-other-rights-under-data-protection-legislation

## INTELLIGENCE DATABASES

29. **Police National Database**
The PND is available to all UK police services and other law enforcement agencies and allows these organisations to share intelligence and other information. The prioritised uses of the PND are the protection of children and young people, understanding and reducing the threat posed by terrorism and disrupting and preventing major, serious and organised crime. The Code of Practice on the Operation and Use of the Police National Database states that:

30. 'The Police National Database (PND) is a national information management system that improves the ability of the Police Service to manage and share intelligence and other operational information, to prevent and detect crime and make communities safer. The PND offers a capability for the Police Service to share, access and search local information electronically, overcoming artificial geographical and jurisdictional boundaries.'[29]

31. **The Code goes on to say:**
'2.1 Policing purposes

The PND is to be used solely for policing purposes. For the purposes of this code, policing purposes are:

- protecting life and property;
- preserving order;
- preventing the commission of offences;
- bringing offenders to justice; and
- any duty or responsibility of the police arising from common or statute law.

2.2 Strategic priorities

The PND enables chief officers to make more informed decisions and better risk assessments, supporting the following areas of policing:

- Protecting children and vulnerable people, by being better able to understand the risk they are facing, and by more thorough vetting of people in positions of responsibility and trust.
- Understanding the threat posed by terrorism of whatever nature, and helping to reduce the risk of terrorist activity.
- Disrupting and preventing major, serious and organised crime, helping to reduce the harm caused by the most dangerous offenders.

29 Code of Practice on the Operation and Use of the Police National Database, Home Secretary, 2010, para 1.1

Chief officers should prioritise the use of the PND accordingly but are free to use the PND for other policing purposes.'

32. The PND has a number of access levels according to the requirements of users. These include General Search Users, Auditors and Administrators. Role Based Access restricts the ability of users to view more sensitive data held on the PND. Furthermore, only specified users may access the PND. The PSNI Service Instruction on National Enquiries lays out how access to the PND can be requested.[30]

33. The PND saves time and effort that would otherwise have been spent transferring data manually. The PND system now handles more than 1.5 billion records and twenty million images. Furthermore, the system has the capacity to serve 12,000 users.[31] PSNI currently hold 120 licences allowing a variety of search facilities. The PND also stores custody images.

34. As of 2019, the PND contains almost 18.5 million facial images of which around 14.5 million are technically suitable and of sufficient quality to be searchable are other types of custody image – e.g. profile shots, or images of scars or tattoos.[32] These facial images can be used for searches with facial recognition technology and has led to significant human rights concerns in England and Wales. PSNI currently do not use facial recognition technology, but the introduction of the technology is being discussed, see Chapter 3.

The PND also can access material from other law enforcement agencies from outside the UK. After a 2017 review into unlawfully held custody images on the PND[33], custody images of persons who were subsequently released without a charge, were deleted and should have also been deleted from local policing databases, including those held by PSNI.

If a custody image is deleted by a force, it should automatically be deleted in the PND too, as the PND custody image store is a copy of data held in local systems.

30 PSNI Service Instruction National Inquiries 2019, https://www.psni.police.uk/sites/default/files/2022-09/International%20Enquiries%2026%20February%202018.pdf

31 https://www.datalynx.net/case-studies/police-national-database/ The PND was set up following the Bichard Inquiry into the Soham murders where issues in police intelligence gathering and sharing were identified.

32 Commissioner for the Retention and Use of Biometric Material, Annual Report 2020, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1036487/E02669527_Biometrics_Commissioner_ARA_2020_Text_Elay.pdf

33 Home Office Review of the Use and Retention of Custody Images 2017, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/594463/2017-02-23_Custody_Image_Review.pdf

However, some forces do not take a proactive approach and delete those images when required but only react when there is a request for deletion.[34] This leaves the (small) chance of a police service getting a match on a PND image search due to the retained custody image of an unconvicted person.

### 35. Access to other databases

Data Protection legislation allows organisations to share personal information if it is needed to prevent or detect a crime, or to catch and prosecute a suspect:

'It is often the case that to prevent or detect crime or to locate an offender we must obtain information from another organisation or share information with them. The legislation allows us to both request and disclose this type of information, lawfully. When we request information from another organisation we must complete a form and send it to the organisation, which may hold the information.'[35]

Significant investigations teams will include a Forensic Case Officer who will provide ideas and guidance on the possibility of intelligence or evidence from other non-police databases. An example would be access to air travel passenger data.

36. Access to some EU databases changed because of the EU exit. The provisions in the Trade and co-operation Agreement (TCA), signed by the UK and EU on 24 December 2020, which set out detailed arrangements to facilitate UK-EU cooperation on a range of EU policing and criminal justice measures.[36] The UK retained access to the Passenger Name Record Directive, to the European Criminal Records Information System (ECRIS) (albeit on a different system) but lost access to the Europol Information System (EIS) and to the Schengen Information System (SIS).[37]

37. Air travel companies are obliged to send data on all air passengers heading from the EU to the UK for processing by law enforcement authorities. In the UK, the surveillance and profiling function is carried out by the UK's National Border Targeting Centre. Equally, data on all passengers travelling from the UK to the EU has to be transmitted to EU member states' Passenger Information Units, in accordance with the 2016 Passenger Name Record Directive.[38]

34 Biometrics and Surveillance Camera Commissioner Annual Report 2021/22, para 83
35 https://www.psni.police.uk/data-protection
36 Beyond Brexit: policing, law enforcement and security, HL Paper 250, House of Lords, European Union Committee, https://publications.parliament.uk/pa/ld5801/ldselect/ldeucom/250/250.pdf
37 See UK EU Trade and Cooperation Agreement, Part Three: Law Enforcement and Judicial Cooperation in Criminal Matters
38 https://www.statewatch.org/news/2022/december/eu-to-approve-further-uk-derogations-from-air-passenger-profiling-safeguards/

38. ECRIS[39] provides for sharing of criminal record data and translates offences between Member States and is essential to connect national criminal databases and facilitate information exchange.[40] As a third country, the UK no longer has access to ECRIS but, at the same time, 'the new system is built on the ECRIS infrastructure for EU member states. It says that the UK must build its own infrastructure and it will interact with a member state's infrastructure, which in turn will be built up on the ECRIS infrastructure.'[41]

39. The EIS is a criminal intelligence and information database holding information on serious international crimes, suspected and convicted persons, criminal structures and offences. As a result of Brexit, the UK is no longer part of Europol. However, to facilitate cooperation, the UK will designate a "national contact point" at Europol. This will act between Europol and the competent authorities of the UK. The national contact point will act as a conduit for information and personal data between Europol and the UK's competent authorities. In addition, the UK will second "one or more" liaison officers to Europol's offices in The Hague, while Europol "may" do likewise to the UK.[42]

40. The SIS is a governmental database maintained by the European Commission. The SIS is used by 31 European countries to find information about individuals and entities for the purposes of national security, border control and law enforcement since 2001. Access ceased in 2021, and the system that UK law enforcement agencies will use instead, the Interpol I-24/7 database, does not yet provide them with the same information at the same speed.[43]

## CONTROLS, ERRORS, AND BREACHES

41. The ICO reported 35 data breach reports from PSNI between 2019 and the end of 2022.[44] How data breaches are dealt with by the PSNI and the risk mitigation in place are addressed in the chapter on Data Protection. Given that police services such as PSNI hold a lot of sensitive data about many people, it is important that this data is adequately protected. This means not just protecting the data from being shared outside of the organisation, but that it's also only accessible to officers or other staff at PSNI who have a reason to see this data.

39 https://commission.europa.eu/law/cross-border-cases/judicial-cooperation/tools-judicial-cooperation/european-criminal-records-information-system-ecris_en
40 Chapter 3, NIHRC, Submission to NI Affairs Committee Inquiry on Cross-border Cooperation on Policing, Security and Criminal Justice after Brexit, September 2020, https://nihrc.org/uploads/publications/NIHRC-NIAC_Brexit_and_Cross-Border_Cooperation-FINAL.PDF
41 https://committees.parliament.uk/oralevidence/1536/html/, see also para 55, Beyond Brexit: policing, law enforcement and security, HL Paper 250, House of Lords, European Union Committee
42 paras. 105 – 111, Beyond Brexit: policing, law enforcement and security, HL Paper 250, House of Lords, European Union Committee
43 ibid. paras 60 - 87
44 ICO, FOI request response, IC-204304, 9 December 2022.

One of the tasks of the Data Protection Officer (DPO) at PSNI is to achieve an understanding of the processing of personal data which occurs across an organisation and to consider if this processing is wholly compliant with legislation, identify where compliance can be strengthened, and risk further mitigated.

## REQUESTING PERSONAL INFORMATION

42. Under Data Protection legislation, everyone has a right to know what kind of personal data is being processed by organisations, including police services. Everyone can make a Subject Access Request to PSNI by completing a Subject Access Request form (DAT1)[45] and emailing it to DataProtection@psni.police.uk.

## REMEDIES FOR CORRECTING INFORMATION

43. The Data Protection Act 2018 provides a number of individual rights:

- the right to be informed;
- the right of access;
- the right to rectification;
- the right to erasure or restrict processing; and
- the right not to be subject to automated decision making.[46]

The Information Commissioner's Office regulates the collection, retention and transfer of personal data and has enforcement powers.

44. People who believe that their data or information about them is held or being accessed by the police have a 'subject access right'.[47] People have the right to ask an organisation whether or not they are using or storing your personal information. People can also ask them for copies of their personal information, verbally or in writing and;

- how they are using it;
- who they are sharing it with; and
- where they got their data from.[48]

45 https://www.psni.police.uk/request/information-about-yourself
46 A Guide to the Data Protection Principles, ICO, accessed at: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-protection-principles/a-guide-to-the-data-protection-principles/
47 See 'Your Data Matters' on the ICO website https://ico.org.uk/your-data-matters/crime/ and the PSNI's procedure https://www.psni.police.uk/request/subject-access-request
48 Part 3, Chapter 3, Data Protection Act 2018.

45. There are, however, issues about adequate redress. Following the Policing Board's Thematic Report on the PSNI's Response to Covid19[49], the PSNI accepted mistakes in the issuing of fixed penalty notices to those involved in the Black Lives Matter protest in June 2020. As a result, the Board was informed that the records created and held on those involved were delated but:

'It should be noted that the Police Service cannot amend information held on our systems that has been created and transferred to our systems by the Northern Ireland Court Service e.g. Court outcomes.'[50]

46. There is provision for deletion or amendment of a criminal history in exceptional circumstances, for example inaccurate information, attributed to the wrong individual, the court outcome is recorded incorrectly, or misspelling of a person's name. Under data protection legislation an individual has the right to obtain from PSNI confirmation as to whether personal data concerning them is being processed and, where that is the case, access to personal data and the following information within one calendar month (this can be extended by a further two months in certain circumstances):

- The purposes of the processing and if processed for law enforcement purposes the legal basis for processing;
- The categories of personal data being processed;
- The recipients or categories of recipient to whom the personal data have been or will be disclosed. Where personal data are transferred to a third country or to an international organisation, the data subject will have the right to be informed of the appropriate safeguards relating to the transfer;
- Where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;
- The existence of the rights which individuals have with regards to how their data is processed; and
- The right to lodge a complaint with the ICO; and
- Where the personal data was not collected from yourself, any available information as to their source; and
- The existence of automated decision-making, including profiling if processed for non-law enforcement purposes.

49 NIPB Thematic Review of the Policing Response to Covid-19, November 2020, https://www.nipolicingboard.org.uk/publication/report-thematic-review-policing-response-covid-19

50 Letter from the Deputy Chief Constable to the Human Rights Advisor, 22 March 2022.

47. It is important to remember that not all personal information is covered and there are exemptions within the data protection legislation which will usually allow PSNI to refuse to comply with an individual's subject access . In particular:

- The prevention and detection of crime; and
- The apprehension and prosecution of offenders; and
- The interests of national security.[51]

## THE FUTURE OF LAW ENFORCEMENT DATABASES IN THE UK

48. In the future there will be a radical reorganisation of law enforcement and biometric databases in the UK.

49. **Law Enforcement Data Service**
The Home Office is planning to replace the PNC with the National Law Enforcement Data Service (NLEDS).[52] The NLEDS is a unified, common database currently being developed by the Home Office National Law Enforcement Data Programme (NLEDP).[53] The new draft College of Policing Code of Practice for the Police National Computer and the Law Enforcement Data Service sets out the 'policing purposes' as:

- protecting life and property;
- preserving order;
- preventing the commission of offences;
- bringing offenders to justice; and
- any duty or responsibility of the police arising from common or statute law, and safeguarding children and vulnerable adults.[54]

50. 'The Law Enforcement Data Service (LEDS) will provide police forces and other law enforcement agencies with the latest, on-demand and joined-up information at the point of need. This will help to prevent crime and better safeguard the public. The Home Office are responsible for the development and management of LEDS infrastructure, which will be hosted using the skills and expertise of a main system data processor ('a processor'). LEDS will be hosted on a cloud-based platform, which will enable LEDS to facilitate requests for data by authorised users of the service. Authorised users process the data in LEDS under a lawful basis or a lawful purpose.

51 PSNI, https://www.psni.police.uk/request/subject-access-request
52 The National Law Enforcement Data Service is abbreviated as NLEDS or LEDS.
53 https://privacyinternational.org/campaigns/uk-law-enforcement-data-service-leds-new-police-megadatabase
54 College of Policing Code of Practice for the Police National Computer (PNC) and the Law Enforcement Data Service (LEDS), accessed at: https://www.college.police.uk/guidance/pnc-and-leds/code-of-practice

LEDS involves multiple system and services, each providing access to separately owned datasets. It is the responsibility of the controller to determine how that data will be processed. The Home Office will manage the data within LEDS, as directed, by the various controllers. The Home Office, as owners of some data, will also be a controller. LEDS will have multiple controllers and data flow processors, acting on behalf of the Controller. Each role will be legally determined and enforced using joint-controller agreements, data processing contracts and where necessary, memorandums of understanding.'[55]

51. Not surprisingly some human rights NGOs are concerned about the development of LEDS.[56] There are other concerns that have also been identified by the National Audit Office:

- 'Five years after the Department established the NLEDS programme in 2016, the programme is already overdue, has yet to deliver the expected services and the total costs to the Department have increased by 68% to £1.1 billion';
- 'The Department and the police have not had a consistent shared understanding of the intended outcomes of the NLEDS programme';
- 'By autumn 2020, the police had lost confidence in the programme and, in response, the Department began a second 'reset', which is still being implemented';
- 'The Department's failure to deliver NLEDS to date means that the increasingly fragile PNC system has not been replaced, bringing greater risks for police operations and requiring the police to bear more cost';
- 'The operational independence of UK police forces is a key challenge for the Department's implementation of national law enforcement programmes such as NLEDS';[57]

52. LEDS was originally going to combine both the PNC and the PND. However, due to the high level of complexity involved in just replacing PNC, PND is now being progressed as a separate dedicated programme until 2031.[58]

55 Law Enforcement Data Service: Data Protection Impact Assessment, Home Office, December 2021.
56 Is over-policing the future? Development of the UK Law Enforcement Data Service', Privacy International, August 2020.
57 The National Law Enforcement Data Programme, Home Office, National Audit Office, August 2021.
58 Accounting officer assessment: National Law Enforcement Data Programme (NLEDP), https://privacyinternational.org/sites/default/files/2020-08/OP1071%20-%2017072019%20Item%208.1%20LEDSHOB%20Open%20Space%20-%20HOB%20Programme%20Briefing_0.pdf

53. **Home Office Biometrics Programme**

Furthermore, the current biometric collections that are used by law enforcement and immigration agencies will be unified in a single database, the Home Office Biometrics Programme. According to the Home Office, this does not mean that this new project will be combining all data into one mega-database. While all the collections of data will be physically in one system, they will be logically separated with role-based access controls (RBAC) allowing user access only to the data and activities they are permitted to access[59]. This system will eventually link in with the Driver Vehicle Licensing Agency, UK Border Agency, UK Visas and Immigration and the Ministry of Defence.[60]

59 17072019 LEDS/HOB Open Space Home Office Biometrics Programme Briefing Paper, https://privacyinternational.org/sites/default/files/2020-08/OP1071%20%2017072019%20Item%208.1%20LEDSHOB%20Open%20Space%20%20HOB%20Programme%20Briefing_0.pdf

60 Biometrics Strategy: Better public services. Maintaining public trust, Home Office, June 2018.

# CHAPTER 3:
# BIOMETRIC COLLECTION, SEARCHING AND RETENTION

## DEFINITION OF BIOMETRIC DATA

54. Biometric data can be defined as 'biological properties, behavioural aspects, physiological characteristics, living traits or repeatable actions where those features and/or actions are both unique to that individual and measurable, even if the patterns used in practice to technically measure them involve a certain degree of probability'.[61] Biometric data irrevocably alters the relation between body and identity, because they allow the characteristics of the human body to be digitised and 'machine-readable'. Such biometric data can then be stored, searched and processed. Sometimes the biometric information captured from a person is stored and processed in a raw form that allows recognising the source it comes from without special knowledge e.g. a photograph of a face, the photograph of a finger print or a voice recording. Other times, the captured raw biometric information is processed in a way that only certain characteristics and/or features are extracted and saved as a biometric template and cannot be easily understood directly by human beings.[62] The statutory regulation of the way in which the police collect, retain and use biometrics in the UK is confined largely to fingerprints and DNA data, such as in the Police and Criminal Evidence Act 1984 (and the Northern Ireland PACE Order 1989). Given the progress in areas such as voice analytics, gait analysis and AI-driven surveillance technology, the legislation is looking increasingly anachronistic. See Chapter 4 for further comments on AI-driven developments.

## BIOMETRICS TAKEN ON ARREST

55. If a person is arrested for a recordable offence and taken to a PSNI custody suite their identity is checked using their fingerprints. Their fingerprints are taken electronically using a 'Live Scan Unit.[63] These are sent automatically to the national fingerprint collection held within IDENT1 and the result is returned to the custody

61 Article 29 Data Protection Working Party, Opinion 4/2007 (WP136, 2007), p. 8., accessed at https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp131_en.pdf

62 Article 29 Data Protection Working Party, Opinion 3/2012 on developments in biometric technologies, accessed at https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp193_en.pdf

63 If a person does not consent to have their fingerprints taken then Article 61 of the Police and Criminal Evidence Order 1989 allows force to be used.

suite within minutes. 'The IDENT1 and Missing Persons' ORD [object-relational database] are the UK databases for the storage, searching, matching and match reporting of fingerprints generated for the UK to provide Metropolitan Police Service - Forensic Services Department with DNA profiles from unsolved crime stains, unidentified body/part(s) and convicted subjects.'[64]

56. The fingerprints are then sent to the PSNI's own Fingerprint Bureau and searched against all unidentified crime scene marks retained on the national database. Finally, if the fingerprints are not already included they will be added to the local and national databases and will then be available for searches by law enforcement agencies across the UK and beyond. DNA samples are also taken at this point. A mouth swab sample using a cotton bud is taken from a prisoner and sent to Forensic Science Northern Ireland. A chemical process is then used to provide a DNA profile which then searched against the Northern Ireland DNA database (NIDNAD) to ascertain whether matching DNA has been recovered from a crime scene. Finally, the profile is added to the national DNA database.[65]

57. As mentioned in the previous chapter, all Biometrics recovered by the PSNI from suspects in the course of an investigation are stored and *speculatively* searched on the following databases:

**Fingerprints**

- National IDENT1 Fingerprint system;
- Paper sets held locally in the PSNI Fingerprint Bureau; and
- National Counter Terrorist Fingerprint Database (NCT FPDB).

64 https://www.gov.uk/government/publications/international-dna-and-fingerprint-exchange-policy-for-the-uk/forensic-information-database-service-finds-international-dna-and-fingerprint-exchange-policy-for-the-united-kingdom-accessible-version

65 'DNA profiles relating to crimes in England and Wales are held on the National DNA Database (NDNAD), managed by the National DNA Database Delivery Unit (NDU) at the Home Office. Each profile records the variation at a defined set of locations (loci) in a person's DNA. The loci that are profiled have been selected because of their suitability for forensic applications and high level of variation between individuals. This variation is due to the difference in the number of times a short sequence of DNA is being repeated over and over again, end to end. The loci are known as short tandem repeat (STR) loci.'
The majority of each person's DNA is normally organised into 23 chromosome pairs. It is expected that a person will inherit one chromosome within a pair from each of their parents, in other words, they will inherit half of their chromosomal DNA from each parent. This means that for each locus there will be a copy of DNA that has originated from each parent, i.e. the loci is normally made up of two DNA components. Statistical methods have been developed to calculate the probability of one DNA profile matching another DNA profile by chance, based on the DNA samples coming people belonging to a large mixed population rather than from people in closer relationships, such as close relatives, siblings or ethnic groups.' DNA-17 Profiling, Crown Prosecution Service.

**DNA**

- Local Northern Ireland DNA Database (NIDNADB);
- National DNA Database (NDNADB);
- National Counter Terrorist DNA Database (NCT DNADB)[66].

58. In the latest annual report by the Biometrics and Surveillance Commissioner, the Commissioner comments on the fact that police in England and Wales routinely search against the Immigration and Asylum Biometric System (IABS) database when someone is fingerprinted solely on the basis that they are technically able to do so, even if there is no link between the person and immigration matters. The IABS database records are much broader than IDENT1 and are held for 10 years.[67] In Northern Ireland a number of NGOs working with victims or witnesses of crime who are not citizens of the UK or the Republic of Ireland are concerned about the lack of clarity on the PSNI's policy on reporting to the immigration authorities. In April 2023 the Policing Board and the PSNI started to work together to try to develop a more transparent policy.

59. Facial images (digital photographs) are also taken of the suspect in custody. The process works as follows: 'Like fingerprints, custody images are taken in the custody suite and can be added to a database; fingerprints are recovered from crime scenes just as images can be recovered from CCTV and photographs and fingerprints are added to a searchable database and crime scene marks searched against this database; similarly custody photographs can be loaded to a searchable database and images recovered from crime scenes can be searched against this database. Both fingerprints and facial images are subjected to computer generated filters to transform these images into numerical expressions that can be compared to determine their similarity…

Once the image has been captured it is loaded into a facial matching system. This system will take the image and transform the image into a series of numerical expressions.

This is done by measuring the distances between fixed points on a face and comparing the measurements between the various points. This then becomes the facial image reference for the person concerned. The quality of lighting, the angle of the face and the quality of the camera used are all of great importance in ensuring that the best possible image is obtained for processing…

66 PSNI Interim Service Instruction Biometric Retention, https://www.psni.police.uk/about-us/our-policies-and-procedures/corporate-policy/service-instructions

67 Biometrics and Surveillance Camera Annual Report – 2021/2022, Office of the Biometrics and Surveillance Camera Commissioner, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1135384/Biometrics__Surveillance_Camera_Commissioner_Annual_Report_21-22.pdf

The image and the information attached to it will be added to the database and it is then ready to be searched against other facial images held. In a police environment these may be other custody images or they may be images obtained from potential crime scenes. The comparison of two custody images should be relatively straightforward as both images have been taken in controlled environments where image quality will have been a priority.'[68]

60. At the present time quality standards for 'facial matching' are less rigorous than for fingerprints and DNA profiles and a definitive match for evidential purposes is more difficult. The planned centralised Home Office Biometrics Strategic Facial Matcher Project will require changes in PSNI processes, particularly for dealing with people taken into custody. In a recent report, the Scottish Police Authority and the Scottish Biometrics Commissioner have highlighted the fact that the low age of criminal responsibility results in children's biometric data being captured upon arrest.[69] Northern Ireland's age of criminal responsibility at 10 years old is even lower than that of Scotland (12 years).

61. Under the Prüm Agreement, a Europe wide agreement on the searching and exchange of biometrics PSNI can search the DNA databases of 15 European states and direct access to the fingerprint databases of Germany, Belgium and Austria and will soon have access to the Czech databases.[70]

## BIOMETRIC RETENTION AND THE NORTHERN IRELAND BIOMETRICS COMMISSIONER

62. In May 2013, the Northern Ireland Assembly passed the Criminal Justice Act (Northern Ireland) 2013 (CJA). Schedule 2 of the Act makes provision for a new regime which sets out a series of rules for the retention of DNA and fingerprints taken by police based on the seriousness of the offence, the age of the person from which the material was obtained, whether the person was convicted or not convicted and the person's criminal history.[71] The CJA has yet to be implemented, for a background explanation of the current problem of biometric retention in Northern Ireland, please refer to Annex B. The legislation also makes provisions for a Northern Ireland Biometrics Commissioner.

68 PSNI Strategic Facial Matcher Project, Project Initiation Document, 6 November 2022.
69 Scottish Police Authority & Scottish Biometrics Commissioner, Joint Assurance Review of the acquisition of biometric data from children arrested in Scotland, 2023, https://www.biometricscommissioner.scot/media/fqkeklo5/final_children_jointassurancereport.pdf
70 PSNI Strategic Facial Matcher Project, Project Initiation Document, 6 November 2022, see also https://www.lawsociety.org.uk/topics/brexit/law-enforcement-and-judicial-cooperation-in-criminal-matters-after-brexit
71 In the meantime, individuals can apply to PSNI to have their fingerprints and DNA taken under PACE removed if there are grounds to do so, see https://www.psni.police.uk/biometric-deletion-requests

63. The Scottish Biometrics Commissioner took up office in 2021 and is an example of how the office of Biometrics Commissioner might be established in Northern Ireland. The Commissioner's 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 for criminal justice and police purposes by Police Scotland, the Scottish Police Authority, and the Police Investigations and Review Commissioner.[72]

64. In February 2019 the ECtHR gave its judgment in a case challenging the retention policies of the PSNI (and of police services across the UK).[73] The Department of Justice held a consultation and intends to change the current legal framework; however it is understood that any new provisions will not be introduced in the Assembly until at least 2025 (the absence of a functioning Assembly contributing to this delay). The Department of Justice proposed to make a provision within CJA to widen the scope of the Northern Ireland Commissioner for the Retention of Biometric Material (the Commissioner) to provide independent statutory oversight of the acquisition, retention, use and disposal of biometric material in accordance with Article 63B to 63R of PACE NI. The Department also wishes to broaden that scope to include keeping under review existing, emerging, and future biometrics for use by the PSNI and other public bodies for law enforcement purposes.[74]

65. Under the current provisions of Schedule 2 of CJA, the Commissioner's sole function was to consider applications from the PSNI for the retention of DNA and fingerprints from persons arrested, but not charged with a serious offence and where so called 'prescribed circumstances' apply. This was to be an exception to the overall retention architecture and was opposed by some MLA Members when the 2013 Act was considered by the Assembly. The retention of biometric material by the PSNI of a person not convicted of an offence is unlikely to comply with Article 8. Currently the PSNI are having to operate a system that is unlawful with all the risks of litigation that this involves, the only permanent solution is for the Assembly to change the law. The Human Rights Advisor has previously made recommendations to PSNI regarding unlawfully retained material, including:

72 https://www.biometricscommissioner.scot/
73 *Gaughran v UK* paras 94 - 96
74 Department of Justice, A consultation on proposals to amend the legislation governing the retention of DNA and fingerprints in Northern Ireland, July 2020, https://www.justice-ni.gov.uk/sites/default/files/consultations/justice/consultation-on-biometrics-provisions.pdf

66. Recommendation 2 in the HRAR 2021/22 stated:

*The PSNI obtain legal advice, which it should provide, in confidence, to the Policing Board's Human Rights Advisor so that it is able to re-write its Service Instruction, delete the unlawfully retained material, and ensure that, as far as possible, it complies with the two ECtHR cases.*

A summary of the issue and background information can be found in Annex B, including the problem of retention of biometric material for legacy investigation purposes.

67. The Department proposed to amend CJA to require the NI Commissioner to report annually, and also as necessary to them and for the Department of Justice to publish and lay reports in the Assembly. This reflects the wider statutory role of the Commissioner for the retention and use of biometric material in England and Wales.

## BEHAVIOURAL VIDEO ANALYTICS SYSTEMS

68. PSNI purchased a behavioural video analytics system for the Muckamore Abbey Hospital Investigation (Operation Turnstone):

'PSNI has procured a behavioral video analytics system in order to be more efficient and accurate in the identification and production of evidence in relation to both suspects and victims, where CCTV or video footage is available. One of the main drivers for this was Operation Turnstone, the Muckamore Abbey Hospital Investigation, which required the allocation of significant officer resource to inspect thousands of hours of CCTV footage.

The analytics system can review video footage sourced from a range of devices in different settings ranging from commercial utility installations to personal devices used socially, typically commercial CCTV systems, dashboard cameras or mobile phones. The system can rapidly 'recognise' individuals in an area of interest but does not identify individuals faces nor is it linked to any other database to enable 'identification' of individuals.'[75]

69. Behavioural video analytics are therefore not to be confused with facial recognition systems and are technically not considered a biometric system.

75 Note to the Policing Board from PSNI, 28th November 2022.

## RETROSPECTIVE FACIAL RECOGNITION

70. These systems use artificial intelligence to compare still facial images of unknown individuals (obtained from CCTV, dash cams, etc.) with a reference image database of known individuals. There is a facial matching capability within the Police National Database (PND) to which the PSNI has access. The PND consists of a large database of custody images (alongside other biometric identifiers), including those added by PSNI. Between October 2021 and September 2022, 292 facial matching searches of the system were conducted by PSNI with 17 of these sent out to PSNI officers involved in investigations.

71. 'The PND facial searching capability was not generally known about within the wider PSNI and the use of this system was stopped once ACC Operational Support Department was made aware that it was occurring in order to establish if adequate governance and accountability measures were in place.'[76]

72. At the time of writing a policy on how and when this system should be used was being developed and the system was likely to be used again from 2023. In principle and, in human rights terms, there are significant differences between the normal role of police officers investigating a crime and looking for evidence of that crime and who have committed it and live time surveillance of significant numbers of innocent citizens.[77]

## LIVE FACIAL RECOGNITION SYSTEMS (LFR)

73. 'LFR involves the real time automated processing of digital images containing the faces of individuals such as images extracted from CCTV systems (both static and mobile), whose facial features are measured by LFR software to produce a biometric template of each image for the purposes of uniquely identifying, individuals. LFR is an example of technologies that process biometric data, a particular type of data that was given specific definition within the DPA 2018.

74. In order to determine a match, biometric templates are extracted from the scanned faces of individuals. In the case of LFR deployment under discussion here, these templates are cross referenced with biometric templates extracted from the scanned faces of individuals on a watchlist. The watchlist is a bespoke gallery of persons of interest created by competent authorities such as the police.

76 Note to the Policing Board from PSNI, 28th November 2022
77 See the evidence from the Biometrics and Cameral Surveillance Commissioner to Parliament's Joint Committee on Human Rights, 22 February 2023.

After a facial match is suggested by LFR processes, human intervention is required to assess whether the match is correct and to determine the appropriate response.'[78]

75. The PSNI assess LFR as:

'… a much more contentious use of the technology and it is this type of usage that has drawn the attention of many civil libertarian groups. This involves the positioning of a camera in a prominent position and the gathering of live footage which is then analysed. Faces are picked out of the footage and searched against a "watch list" of images that have been complied on the basis of intelligence. This technology is used extensively on private property such as shopping centres and airports where individuals can be tracked and apprehended if necessary; the use of Live Facial ID on private property has generally not been challenged by individuals or groups, presumably because it is on private property and not in the public domain and used for policing purposes. South Wales Police and the Met have attracted significant attention in the past few years after their use of this technology was made public and they were challenged in the court over their application of it.'[79]

76. South Wales Police had used LFR since May 2017 and may have taken sensitive facial biometric data from 500,000 people without their consent. A resident brought a case against South Wales Police, arguing the force was breaching rights to privacy, data protection laws, and equality laws by taking his biometric data at a protest without his consent. In September 2019, the High Court decided that while facial recognition does interfere with the privacy rights of everyone scanned, the current legal framework provides sufficient safeguards. He appealed the decision, and in August 2020, the Court of Appeal found South Wales Police's use of facial recognition technology breaches privacy rights, data protection laws and equality laws.[80]

77. Following the Court of Appeal judgment, the Met continue to test facial recognition systems using mobile vans:

78 The use of live facial recognition technology by law enforcement in public places, the Information Commissioner, 31 October 2019. See also College of Policing, Live Facial Recognition, 2021 and Governing Live Automated Facial Recognition Systems for Policing in England and Wales, Fengyu (Isabella) Duan, University of Cambridge, December 2020.

79 PSNI Facial Initiation Project, Project Initiation Document, 6 November 2022.

80 https://www.libertyhumanrights.org.uk/issue/legal-challenge-ed-bridges-v-south-wales-police/

'LFR cameras are focused on a specific area; when people pass through that area their images are streamed directly to the LFR system.

This system contains a watchlist: a list of offenders wanted by the police and/or the courts, or those who pose a risk of harm to themselves or others…

The Met is testing its facial recognition algorithms with the National Physical Laboratory (NPL)…

This testing will further enable us to understand more about the algorithm's accuracy and if any biases have been detected. The data for these tests needs to be collected in a realistic operational policing environment and therefore this data will be collected whilst a number of LFR deployments are happening. The results of this testing will help inform the Met how we use facial recognition technology legally and fairly in order to prevent and detect crime, safeguard national security and keep Londoners safe.'[81]

78. In relation to safeguards and protections the Metropolitan Police have set out the position as follows:

'For the MPS to use LFR in a lawful and ethical manner we acknowledge the need to adopt safeguards that sufficiently mitigate the impact that LFR has on Article 8 rights. We also recognise that LPEP [London Policing Ethics Panel] set out five conditions that they considered necessary to support the ethical use of LFR in a law enforcement context:

- The need to demonstrate LFR is of more than marginal benefit;
- Building trust by making trial data public;
- Necessity and proportionality;
- Focused training for police civilian operators and officers; and
- Robust voluntary self-regulation with independent oversight.'[82]

79. According to experts, 'computer vision' is still very inaccurate and we are perhaps a decade or even two away from cameras accurately identifying faces. On top of that, these high-tech cameras require large amounts of storage, which poses a logistical problem. However, the rapid technological advancement of surveillance technology means that safeguards and human rights considerations must 'grow' equally and be implemented alongside with these technologies.

81 https://www.met.police.uk/advice/advice-and-information/fr/facial-recognition/

82 Letter from the MPS to the London Mayor, 23 January 2020. See also its detailed policy document on its use of this technology, https://www.met.police.uk/SysSiteAssets/media/downloads/force-content/met/advice/lfr/policy-documents/lfr-policy-document.pdf

80. The Met seems confident in the facial recognition trial outcomes.[83] An independent academic report on the trials that were conducted from 2016 – 2019 has highlighted the following:

'MPS officers considered the LFR match sufficiently credible to stop individuals and perform and identity check on 26 occasions. Four of these attempted interventions were unsuccessful. Usually this was because the individual became lost in a crowd. Of the remaining 22 stops, 14 were verified as incorrect matches following an identity check. Eight verified as correct matches following an identity check.'[84]

This constitutes a success rate of 36%.

81. A new feasibility study that was published in March 2023 reports that accuracy levels in facial matching have improved.[85] However, the watchlist used for the study was 'an order of magnitude larger than typical for an MPS [Metropolitan Police Service] LFR deployment. The watchlist contained nearly 180,000 facial images, which is about 20 times the size of any watchlist used operationally to date.'[86] Human rights NGOs have criticised the new study, highlighting that the important question is how this technology is being used: 'Facial recognition doesn't make people safer, it entrenches patterns of discrimination and sows division.'[87]The Biometrics and Surveillance Camera Commissioner has issued guidance on using FRT to locate persons on a watchlist. The guidance states that police services should put policies in place which guard against an 'impermissively wide area of discretion' afforded in the selection of those who are to be placed upon a watchlist and to the selection of the location(s) where the use of LFR is to take place. Watchlists should also not be simply copied between operations.[88]

83 https://www.met.police.uk/SysSiteAssets/media/downloads/central/services/accessing-information/facial-recognition/met-evaluation-report.pdf

84 Fussey & Murray, Independent Report on the London Metropolitan Police Service's Trial of Live Facial Recognition Technology, University of Essex, 2019: https://repository.essex.ac.uk/24946/1/London-Met-Police-Trial-of-Facial-Recognition-Tech-Report-2.pdf

85 Facial Recognition Technology in Law Enforcement Equitability Study Final Report, National Physical Laboratory, March 2023, para 1.4.1

86 Ibid. p. 9

87 https://www.libertyhumanrights.org.uk/issue/liberty-responds-to-release-of-research-into-facial-recognition-technology/

88 Facing the Camera. Good Practice and Guidance for the Police Use of Overt Surveillance Camera Systems Incorporating Facial Recognition Technology to Locate Persons on a Watchlist, in Public Places in England & Wales, Biometrics and Surveillance Camera Commissioner, November 2020

82. Furthermore, images recovered from CCTV systems are not always of very good quality and that is problematic and may result in false positives (and false negatives) if those images of individuals are compared with facial images on databases. It may be relatively easy for an algorithm to accurately assess good images in controlled surroundings but it is likely to be necessary for human intervention to make matching decisions where images are poorer. Use of facial recognition by the MPS and others has raised questions about the systems' ability to accurately match non-European and non-white faces.[89]

## REGULATION

83. There have been considerable concerns in the past about the lack of controls and regulation of CCTV but now the Data Protection Act 2018 applies; the Information Commission has a key role; there is a Home Office, Surveillance Camera Code of Practice[90] and; a Surveillance Camera Commissioner, who has produced a Good Practice Guide.[91] This last role was merged with another role to become the Biometrics and Surveillance Camera Commissioner in February 2022.[92] However, although the biometrics part of this role applies across the UK and includes Counter Terrorist biometric material in Northern Ireland, the Camera Surveillance role is restricted to England and Wales. Furthermore, the Camera Surveillance part of the role is due to be abolished if the proposed changes to the data protection regime are agreed by the Westminster Parliament.[93]

84. Generally speaking, police officers are not entitled to use any surveillance techniques unless the technique is authorised by the law. The procedures must, therefore, comply both with the specific UK laws which apply directly in Northern Ireland and with Article 8 of the ECHR as set out in the Human Rights Act 1998. This means that if the procedure interferes with a person's privacy then the aim of the interference must be legitimate, it must be sanctioned by the law and it must be proportionate.[94]

85. As is clear these interests or 'legitimate aims' are quite wide-ranging but the additional and key part of the justification for any interference with this right, is the requirement of proportionality – it must be necessary to achieve the aim in question.

89 Countermeasures: the need for new legislation to govern biometric technologies in the UK, Ada Lovelace Institute, June 2022. See also section 1.5, College of Policing, Facial Recognition, 2021.
90 For England and Wales published by the Home Office, November 2021.
91 Facing the Camera: Good Practice and Guidance, November 2020.
92 https://www.gov.uk/government/organisations/surveillance-camera-commissioner
93 Data Protection and Digital Information (No 2) Bill, https://bills.parliament.uk/bills/3430
94 Regarding public surveillance, issues of public consent and the Right to Freedom of Expression and the Right to Assembly are engaged, however, these are not considered in this report.

In practice, the greater the interference with privacy, the greater the justification must be and that principle must be set out clearly in the policy or code that controls its use in practice.

86. In addition, to including this proportionality principle, the law setting out any surveillance power has to be transparent, precise and provide strict checks and balances. For instance, in the recent case about a live facial recognition system being used by the South Wales Police, the High Court explained what those legal requirements must be:

a. The measure in question (a) must have 'some basis in domestic law' and (b) must be 'compatible with the rule of law' …
b. The legal basis must be 'accessible' to the person concerned, meaning that it must be published and comprehensible, and it must be possible to discover what its provisions are. The measure must also be 'foreseeable' meaning that it must be possible for a person to foresee its consequences for them ....
c. The law must 'afford adequate legal protection against arbitrariness …
d. …. (b) what is required is that 'safeguards should be present in order to guard against overbroad discretion resulting in arbitrary, and thus disproportionate, interference with Convention rights'. Any exercise of power that is unrestrained by law is not 'in accordance with the law'.[95]

87. The key messages in the Opinion given by the Information Commissioner on LFR are as follows:

- 'The use of LFR involves the processing of personal data and therefore data protection law applies, whether it is for a trial or routine operational deployment.
- The processing of personal data by 'competent authorities' (s30 DPA 2018) for 'the law enforcement purposes' (s31 DPA 2018) is covered by Part 3 of the DPA 2018.
- Specifically, the use of LFR for the law enforcement purposes constitutes 'sensitive processing' (s35 (8)(b) DPA 2018) as it involves the processing of biometric data for the purpose of uniquely identifying an individual.
- Such sensitive processing relates to **all** facial images captured and analysed by the software; and must pay particular attention to the requirements of s35, s42 and s64 DPA 2018. As such, a Data Protection Impact Assessment (DPIA) and an 'appropriate policy document' must be in place.

95 para 55, R v The Chief Constable of South Wales Police & others [2020] EWCA Civ 1058, accepted by the parties see para 56.

- Sensitive processing occurs **irrespective** of whether that image yields a match to a person on a watchlist or the biometric data of unmatched persons is subsequently deleted within a short space of time.
- Data protection law applies to the whole process of LFR, from consideration about the necessity and proportionality for deployment, the compilation of watchlists, the processing of the biometric data through to the retention and deletion of that data.
- Controllers must identify a lawful basis for the use of LFR. This should be identified and appropriately applied in conjunction with other available legislative instruments such as codes of practice.
- The Commissioner intends to work with relevant authorities with a view to strengthening the legal framework by means of a statutory and binding code of practice issued by government. In the Commissioner's view, such a code would build on the standards established in the Surveillance Camera Code (issued under the Protection of Freedoms Act (POFA 2012) and sit alongside data protection legislation, but with a clear and specific focus on law enforcement use of LFR and other biometric technology. It should be developed to ensure that it can be applicable to current and future biometric technology.' [96]

88. It is important to note that there are some circumstances where the use of *available* LFR technology would not only be useful for policing purposes[97] but might engage the positive obligations of a state under Article 3 of the ECHR (the prohibition of ill-treatment) as set out in *O'Keeffe v Ireland*[98] and considered in *Commissioner of Police for the Metropolis v DSD*[99]. If a police service has access to LFR technology which might help in a criminal investigation into alleged serious ill-treatment, then that technology needs to be used. Increasingly, police forces are also relying on citizen-generated images (Go-Pros, home security systems, dashcams etc.), which members of the public share with them. Video analytics capabilities mean that this data can be put to practical use, but the retention, comparison and even sharing with other jurisdictions is only subject to the general data protection rules and is therefore out of step with the regulation of biometrics such as fingerprints and DNA. Before the advent of current sophisticated video analytics technology, there was simply too much material to comb through, but now police services and other public authorities are now able to tap into an aggregated surveillance capability that is vast and growing.[100]

96 The use of live facial recognition technology by law enforcement in public places, 31 October 2019.
97 See for example https://techmonitor.ai/policy/privacy-and-data-protection/facial-recognition-needs-stronger-case-law-enforcement
98 [2014] ECHR 96
99 [2018] UKSC 11
100 Office of the Biometrics and Surveillance Camera Commissioner, Annual Report 2021/22, para 122.

89. **PSNI's use of facial recognition technology**

In light of these concerns, the Policing Board made the following recommendation in the Human Rights Annual Report for 2020/21:

*'The PSNI should consult the Policing Board and the wider public if facial recognition technology is to be recommended to assist in preventing crime or investigating offences and this should be subject to an equality impact assessment and human rights audit.'*

90. The PSNI accepted this recommendation and stated:

'The Police Service of Northern Ireland does not currently operate a Facial Identification System but fully recognises the value this could bring to investigations and public safety. We also recognise the need for robust governance around its use. To that end the Police Service is closely engaged with the Home Office Biometrics Programme who have plans to develop a National Facial Identification system. The Service will be invited to sit on the Home Office Biometrics Facial Matching Project Board, charged with delivering a National Facial Identification system and will contribute to its development.

91. However, this system will be based on using retrospective facial images, rather than the live facial images that have resulted in the recent legal challenge involving South Wales Police. As the national system develops the Police Service of Northern Ireland will fully consult with the Policing Board, Human Rights Commission and the public as the technology advances and will ensure equality assessments are completed. The Police Service's desire is to ensure that there is a full transparency and governance around the use, sharing and retention of facial images.

92. The Head of Forensic Services now sits on the Home Office Strategic Facial Matching (SFM) Project Board. The HO SFM Board are currently developing a communication package for potential stakeholders including PSNI, DoJ and the Policing Board to provide clarity around the development of a national system. A Project Board will commence in September to start exploring facial identification in consultation with the Policing Board.'[101]

101 Recommendation 6, Human Rights Annual Report 20/21.

93. This PSNI Facial Identification Project Board was established in September 2022 to ensure any new facial identification technology being considered by the Home Office Biometrics Strategic Facial Matching Project would be introduced to PSNI in a controlled manner ensuring full consultation, compliance with human rights, and governance are in place in advance.[102] In 2022, the Community Rescue Service (CRS) set up a CCTV system in Coleraine with the 'primary objective of locating missing and vulnerable people.' This system had facial recognition capability, including the facility to carry out live-time searches. PSNI were initially uncertain of the extent of PSNI influence in the CRS CCTV system in Coleraine but a review through the Facial Identification Project Board indicated that PSNI had no direct input. The Human Rights Advisor attended the Facial Identification Project Board in January and March 2023 and continues to be involved as discussions within PSNI take place. PSNI are currently developing Guidance on Usage of Retrospective PND Facial Searching, and the Human Rights Advisor has seen the draft guidance and provided feedback.[103]

102 Note to the Policing Board, 28th November 2022.
103 Letter from Human Rights Advisor John Wadham to ACC Chris Todd, 29 March 2023.

# CHAPTER 4:
# ARTIFICIAL INTELLIGENCE

94. The term AI can often induce fear – or perhaps wonder – as it seems like it is going to take over the world at any moment. Considering that there is no agreement on the definition of AI, and that the technology which can be understood under this umbrella term is changing at a fast pace, it is difficult to pinpoint what artificial intelligence really is. Applications range from social media algorithms, phenomena such as ChatGPT[104] to its use in public decision-making and medical settings – not all of them successful or lawful.[105] At its simplest form, artificial intelligence is a field which combines computer science and robust datasets to enable problem-solving. It also encompasses sub-fields of machine learning and deep learning, which are frequently mentioned in conjunction with artificial intelligence. These disciplines are comprised of AI algorithms which seek to create expert systems which make predictions or classifications based on input data.[106] As Meredith Broussard stated, 'the problem starts when people think AI is smarter than it is'.[107] One could argue that this is the case with the current state of Live Facial Recognition technologies – as this report highlighted in the previous chapter, the match rate in the Met trials was very low.

95. Apart from the retrospective facial recognition system used for the Muckamore Abbey investigation, PSNI selectively employ some tools that make use of artificial intelligence, such as a software tool used for online research purposes. The PSNI officers that the Human Rights Advisor spoke to in preparation of this report clarified that AI technology would never be involved in decision making and that the technological advances that AI is making, means that all law enforcement agencies are grappling with the problem of if and how to use these technologies. One of the issues where AI could be useful is data processing – a tool that would help process data, as the volume and complexity of data in investigations is steadily increasing. A PSNI officer explained that: 'AI appears to be particularly good at categorising large quantities of images for further analysis by a human operator. This saves significant amounts of time and reduces the likelihood of relevant material being overlooked. Please note this does not currently include the use of facial recognition technology.'[108]

104 https://openai.com/blog/chatgpt/
105 https://www.theguardian.com/technology/2020/feb/05/welfare-surveillance-system-violates-human-rights-dutch-court-rules
106 https://www.ibm.com/uk-en/topics/artificial-intelligence
107 Meredith Broussard, Artificial Unintelligence: How Computers Misunderstand the World.
108 Letter from PSNI to the Human Rights Advisor, 14 February 2023.

96. PSNI is, however, involved in several European projects aimed at improving the delivery of policing in various aspects.[109] One of them is the ROXANNE project[110], which makes use of speech processing technologies, natural language processing, video and geographical meta-data processing and network analysis to combat organised crime network – all artificial intelligence technologies that have the potential to greatly assist police services in their work. ROXANNE stands for Real time netwOrk, teXt, and speaker ANalytics for combating orgaNized crime. There are three main sources of data for technical training, development and evaluation activities in ROXANNE: data from the law enforcement agencies, such as anonymised data from old cases, publicly accessible media, and research activities.[111] One of the main challenges identified by the project was the sheer volume of data that law enforcement agencies had to process. The ROXANNE platform is open-sourced for European law enforcement agencies and will automate time-consuming tasks. Law enforcement agencies from Greece, Germany, the Republic of Ireland, Romania, Lithuania, Israel, the Czech Republic and others participated in the project.[112] Among the industry partners are Airbus and Interpol. PSNI has previously been criticised for its involvement in the project, given Israel's human rights record.[113]

97. As a College of Policing document illustrates, AI has the potential to vastly improve policing's ability to prevent crime, manage its resources more efficiently and coordinate fast-moving responses to major incidents. Crime prevention and criminal investigation teams could use AI to speed up the identification of criminals and their motives; neighbourhood policing teams could benefit from a better understanding of community dynamics; major incident commanders could use AI systems to improve situational awareness and better visualise potential strategies and tactics; and police call centres could use AI systems such as those pioneered by Amazon and UPS to more efficiently route responses to calls for service.[114]

98. However, these technologies also pose risks if not properly regulated and have the potential to seriously infringe on privacy rights and the right to freedom from discrimination – a concern that is woven throughout this report and addressed in the concluding chapter. The way in which new AI-driven technology such as LFR

109 https://www.psni.police.uk/safety-and-support/advice-and-information/eu-funded-research-projects
110 https://www.roxanne-euproject.org/project
111 https://www.roxanne-euproject.org/results/files/d4-1.pdf
112 https://www.roxanne-euproject.org/consortium
113 https://www.thedetail.tv/articles/psni-partnership-with-israeli-police-and-prisons-ministry, https://www.amnesty.org.uk/press-releases/northern-ireland-psni-must-end-work-israeli-police-and-security-services
114 College of Policing (2020) Our Policing in England and Wales: Future Operating Environment 2040, accessed at: https://assets.college.police.uk/s3fs-public/2020-08/Future-Operating-Environment-2040-Part1-Trends.pdf

is used by the police is only part of the challenge however, the way in which it is *perceived* to being used, particularly against some communities may be every bit as important as its technological accuracy.[115]

99. One of the developments that hasn't been addressed by current or proposed legislation is Biometric classification or categorisation technology, which can be very problematic. This technology uses AI for the purpose of assigning natural persons to specific categories, such as sex, age, hair colour, eye colour, tattoos, ethnic origin or sexual orientation, on the basis of their biometric data.[116] Other software aims to recognise and classify emotions. One of the reasons why these classification and prediction technologies are particularly problematic is the 'black box' problem - humans don't really understand how a complex algorithm comes to a decision or result.[117] This affects all technologies that use algorithms but is particularly problematic when algorithms make decisions that impact people's lives.[118] These capabilities have not been addressed by proposed UK legislation but are addressed in the proposed EU AI Act.[119] At the time of writing the UK Government was about to produce a White Paper setting out its approach to AI use in the future. An alternative accountability framework proposal already exists: The Accountability Principles for AI in law enforcement (AP4AI)[120] is the first comprehensive framework providing decision makers with guidance at all levels of accountability in policing. It was developed in close consultation with Europol and the EU Fundamental Rights Agency, and was presented to PSNI in 2022.

115 p. 40 Countermeasures, Ada Lovelace Institute, https://www.adalovelaceinstitute.org/wp-content/uploads/2022/06/Countermeasures-the-need-for-new-legislation-to-govern-biometric-technologies-in-the-UK-Ada-Lovelace-Institute-June-2022.pdf

116 Ibid. p. 16 - 20

117 Solving the Black Box Problem: A Normative Framework for Explainable Artificial Intelligence Carlos Zednik, https://arxiv.org/ftp/arxiv/papers/1903/1903.04361.pdf#:~:text=The%20Black%20Box%20Problem%20is,problems%20in%20AI%20are%20opaque.

118 https://www.adalovelaceinstitute.org/wp-content/uploads/2022/06/Countermeasures-the-need-for-new-legislation-to-govern-biometric-technologies-in-the-UK-Ada-Lovelace-Institute-June-2022.pdf

119 https://artificialintelligenceact.eu/the-act/

120 https://www.europol.europa.eu/cms/sites/default/files/documents/Accountability_Principles_for_Artificial_Intelligence_AP4AI_in_the_Internet_Security_Domain.pdf

# CHAPTER 5:
# GENERAL SURVEILLANCE

100. A case against the UK in the ECtHR highlights how surveillance can be a force for good in certain cases, but the use of it needs to be regulated and individuals' privacy needs to be protected, even in public spaces.[121] A man suffered from depression and was filmed by the Council CCTV system with a kitchen knife in his hand with which he attempted to harm himself. The control room operator was alerted to an individual in possession of a knife. The police were notified and arrived at the scene, where they took the knife, gave the applicant medical assistance, and brought him to the police station, where he was detained under the Mental Health Act 1983. However, the Council released the footage to the broadcast and print media with the result that it appeared on TV and in the local press. After complaining to several broadcasting commissions and the domestic courts the man took his case to the ECtHR.

101. The ECtHR ruled that his right to private life had been violated. Among other things, the applicant was not informed before and had not consented to the disclosure of the footage. The UK Press Complaints Commission previously rejected the applicant's complaints because the events in question occurred in a public place, but the ECtHR summarily rejected this argument. The case highlights the positive impact of CCTV – a person suffering from mental ill-health was prevented from ending their life and helped – but also illustrates that in public places, privacy protections still apply. This principle is even more important now in an era of ubiquitous CCTV coverage[122] and the advent of facial recognition technology, than it was in 1995.

## VIDEO SURVEILLANCE

102. **Legal Basis**

The recording of persons by law enforcement personnel or accessing recordings are generally lawful under international human rights law, subject to the requirement that:

- the interference with rights is based on law (i.e. clear, foreseeable and accessible);
- pursues a legitimate aim;

121 Application number 44647/98, 28 January 2003.
122 https://www.cctv.co.uk/how-many-cctv-cameras-are-there-in-london/

- is proportionate to that aim; and
- necessary in a democratic society.

103. The lawful collection and use of personal data for law enforcement purposes is important for the prevention of crime, maintenance of public order and in the interests of national security. However, the 'Practical Guide on the Use of Personal Data in the Police Sector' produced by the Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data provides that:

'All data processing has to comply with the necessity, proportionality and purpose limitation principles. This implies that personal data processing within the police should be based on predefined, clear and legitimate purposes set out in the law; it should be necessary and proportionate to these legitimate purposes and should not be processed in a way incompatible with those purposes. Data processing should be carried out lawfully, fairly and in a transparent manner. Personal data within the police should furthermore be adequate, relevant and non-excessive in relation to the purposes. Finally they should be accurate and up-to-date to ensure the highest data quality possible.'[123]

104. While being in a public area may mean enjoying a lesser degree of privacy, individuals should not be deprived of their rights. According to the Public Order (Northern Ireland) Order 1987, "public place" means any highway and any place to which at the material time the public or any section of the public has access, on payment or otherwise, as of right or by virtue of express or implied permission.[124]

105. The Protection of Freedoms Act 2012 introduced a wide range of measures regarding the regulation of surveillance and other state powers. Part 2 Chapter 1 introduces a code of practice for surveillance camera systems and provides for judicial approval of certain surveillance activities by local authorities. The Surveillance Camera Code of Practice was published in 2013 and last amended in 2021.[125] This Code of Practice provides guidance on the appropriate and effective use of surveillance camera systems by relevant authorities, such as in England and Wales, including law enforcement and councils who operate CCTV.

123 Council of Europe T-PD(2018)01 Consultative Committee Of The Convention For The Protection Of Individuals With Regard To Automatic Processing Of Personal Data. Practical guide on the use of personal data in the police sector. Accessed at https://rm.coe.int/practical-guide-use-of-personal-data-in-the-police-sector/1680789a74

124 Section 2(2) of the Public Order (Northern Ireland) Order 1987.

125 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1010815/Surveillance_Camera_Code_of_Practice__update_.pdf

The Code of Practice contains 12 guiding principles which (if followed) will mean cameras are only ever used proportionately, transparently and effectively (surveillance cameras include CCTV, ANPR, body worn video (BWV) and drone systems).

106. The legislation also established a Surveillance Camera Commissioner, whose role was to promote compliance by police and local authorities.[126] There is no specific guidance for Northern Ireland, however PSNI adheres to this Code of Practice and have been certified by the Surveillance Camera Commissioner.[127]

107. To note, recording, retaining, and revealing of material obtained in a *criminal* investigation, such as CCTV or ANPR material, is governed by the Criminal Procedure and Investigations Act 1996 and the corresponding Code of Practice.[128]

108. **CCTV technology**

The majority of CCTV cameras present throughout Northern Ireland and GB are not operated by the police, but rather by the private sector and public authorities, such as councils and transport authorities. A CCTV camera picks up a sequence of images which are transmitted as a signal to a recording device and displayed on a screen. The signals are not publicly broadcasted, hence the term closed-circuit, and are only accessed by authorised individuals. Both the recorded and live footage can be viewed by them for surveillance and monitoring. Analogue CCTV cameras (coaxial-cabled closed circuitry) record images to a digital recorder which converts the video to a digital format. To view the video, the video recorder needs to be connected to a monitor or router to be broadcast through an internal network for remote access. Digital CCTV cameras or internet protocol cameras, which are much more common these days, record in a digital format so a conversion process is not required. The digital data is sent to a dedicated network video recorder through the existing network and can be accessed remotely.

109. Most modern CCTV cameras are manufactured by Chinese companies, for example Hikvision and Dahua. These modern cameras not only record images but have additional capabilities, such as face detection and facial recognition,

126 This office has now been merged into the Office of the Biometrics and Surveillance Camera Commissioner but legislation in the UK Parliament is designed to reduce the remit of this role.

127 https://www.psni.police.uk/sites/default/files/2022-09/Certificate%20Of%20Compliance%20Police%20Service%20Of%20Northern%20Ireland_1.pdf

128 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/447967/code-of-practice-approved.pdf

gender and age recognition and heat mapping.[129] According to research by Big Brother Watch, 'Hikvision and Dahua are primarily responsible for the normalisation of high-level video analytics for even basic CCTV systems in the UK …. Whilst CCTV operators are obliged to disclose sensitive data processing in a Data Protection Impact Assessment, there is little oversight of this requirement and in practice it is difficult to discover where such capabilities may be in use.'[130]

110. In Northern Ireland, at least 10 out of 20 councils use these cameras.[131] PSNI have audited their CCTV estate for these cameras after the issue was identified by the UK Government in Dec 2022. PSNI had a very small number (less than 10) of them on closed sites with no public access and which were not connected to the internet. None of these types of cameras have any advanced capabilities (face detection/facial recognition/gender or age recognition/heat mapping) and PSNI have also committed to replacing them at the earliest opportunity in line with UK Government recommendations.

111. The Biometrics and Surveillance Camera Commissioner has highlighted the possible human rights issues arise from the use of these cameras in his April 2022 letter to the Minister for the Cabinet Office and the Cabinet Secretary:

'In terms of security, public space surveillance is increasingly intrusive and modern surveillance cameras are built with the maximum functionality inside at the point of manufacture. This means they come with capabilities that can be switched on remotely in the future as and when they are needed, for example, the ability to pick up sound or read vehicle number plates. The more that surveillance camera systems can do, the more important it will be to reassure people about what they are not doing, whether that is in our streets, our sports grounds or our schools. This is increasingly difficult to detect technically and requires transparency and due diligence by all concerned in public space surveillance activity.'[132]

129 Not every type of camera possesses advanced capabilities, which depends on the type of software that is installed. However, sophisticated Hikvision and Dahua software and camera models possess the following capabilities: facial recognition, gender and age recognition, expression and emotion detection, clothes and glasses detection, heat detection, and sorting footage by event type for example. Big Brother Watch, Who's Watching You? The Dominance of Chinese state-owned CCTV in the UK, 2022 https://bigbrotherwatch.org.uk/wp-content/uploads/2022/02/Whos-Watching-You_The-dominance-of-Chinese-state-owned-CCTV-in-the-UK-1.pdf p.11

130 ibid.

131 ibid. p 41

132 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1070869/Letter_from_Biometrics_and_Surveillance_Camera_Commissioner_to_Minister_for_the_Cabinet_Office_and_Cabinet_Secretary_21_April_2022.pdf

112. As of 24 November 2022, the UK Government has 'instructed [departments] to cease deployment of such equipment onto sensitive sites, where it is produced by companies subject to the National Intelligence Law of the People's Republic of China'.[133] In order to be effective (and therefore competitive) facial recognition algorithms need to be 'trained' on the greatest diversity of physiognomy in a 'live' setting. This requires access to large numbers of faces in real time which is why several Chinese companies have supplied and installed state-of-the-art FR cameras to countries in Africa and Europe without cost; the value is in the range and scale of live data passing by. How far citizens are even aware of, still less supportive of this data harvesting of their features is unclear.

113. The Scottish Government has also removed Hikvision cameras from all Government buildings. Denmark, the UK and the USA have all banned Hikvision and in 2021, the European Parliament also removed Hikvision cameras. According to Hikvision's annual report, the company is contracted to operate Chinese state surveillance of Uyghur Muslims. This surveillance system operated by Hikvision targets Uyghurs based on racial attributes and flags them for detention at mass internment camps.[134] In February 2023, Irish Council for Civil Liberties (ICCL) wrote to the Oireachtas to highlight how Hikvision is involved in human rights violations against Uyghur Muslims in Xinjiang and the national security concerns for any state using Hikvision CCTV cameras.[135]

114. In his November 2022 letter to the Security Minister the Surveillance Camera Commissioner highlights the problem of private ownership of advanced technological capabilities:

'As almost all of our technological capability is in private ownership, the people we trust (police, emergency services, local and national government) must be able to trust their surveillance partners or we are in a lot of trouble, not just as a sector but as a society. Trust in this context means a preparedness to take part in a minimum level of public scrutiny, whether that is of your products and services or your trading history, values and principles. If, like some surveillance companies with which I am currently dealing, entities are unwilling to accept that scrutiny and accountability, that is a business decision for them but it is one that, in my view, ought to disqualify them from working in trusted partnership with our democratic institutions.'[136]

133 Security Update on Surveillance Equipment Statement made on 24 November 2022, accessed at: https://questions-statements.parliament.uk/written-statements/detail/2022-11-24/hlws376

134 Irish Council for Civil Liberties, Letter to the Houses of the Oireachtas Commission, 10 February 2023, accessed at: https://www.iccl.ie/news/iccl-calls-for-immediate-removal-of-hikvision-cameras-from-oireachtas/

135 Letter from the Biometrics and Surveillance Camera Commissioner to the Security Minister, 14 November 2022, accessed at: https://www.iccl.ie/wp-content/uploads/2023/02/20230210-ICCL-Letter-Hikvision-Oireachtas.pdf

136 https://www.gov.uk/government/publications/letter-from-the-commissioner-to-the-security-minister/letter-from-the-biometrics-and-surveillance-camera-commissioner-to-the-security-minister

115. **Public space CCTV network in Northern Ireland**
Around 120 Genetec CCTV cameras are installed in Belfast City Centre, which are owned and operated by PSNI. They are monitored around the clock by contracted G4S staff. These CCTV cameras have advanced capabilities, such as Facial Recognition and ANPR, however these capabilities are not being used.

116. Belfast Harbour Police also operates CCTV cameras, and an agreement exists between PSNI and Belfast Harbour Police to access each other's systems if necessary. In Lisburn & Castlereagh, the CCTV system in Lisburn City Centre is owned and operated by the council, with the control room located inside Lisburn police station. In Newry, Mourne, and Down, the camera infrastructure and maintenance is provided by the council, whereas PSNI provide the control room and monitor the cameras through contracted G4S staff. In Mid-Ulster, only CCTV cameras around police stations. Footage is usually kept for 30 days. In Derry and Strabane, the CCTV infrastructure is owned and managed by the council, and PSNI contribute around £50,000 a year to it. There are procedures in place regarding PSNI's access to the CCTV footage.

117. **PSNI's use of CCTV footage**
During a criminal investigation, police may seize and view CCTV footage from private businesses or public authorities (but usually do so with the consent of the operator). PSNI adhere to the Authorised Professional Practice (APP) of the UK College of Policing in their policy regarding CCTV. CCTV is considered a 'passive data generator.[137] Passive data generators are automated systems that gather and collate information for purposes unconnected with criminal investigation but can be accessed by investigators. Examples include:

- financial information;
- CCTV;
- other digital images;
- computer-based electronic evidence;
- telecommunications information; and
- customer information, including subscriber information.

118. APP states that 'Investigators should also take account of the provisions of the Human Rights Act 1998, notably Article 8, respect for private and family life.' Furthermore, the guidance states that investigators be aware of the relevant legal basis for seizing and viewing CCTV, namely:

137 https://www.college.police.uk/app/investigation/investigative-strategies/passive-data-generators

- Criminal Justice and Police Act 2001;
- Criminal Procedure and Investigations Act 1996 (CPIA);
- PACE;
- Police Reform Act 2002; and
- Data Protection Act 2018 (DPA).

119. In practice, most victims of a crime that have access to CCTV will voluntarily hand over footage to PSNI, such as private businesses and individuals that have home cameras installed. Due to the sheer volume of the data accumulated, PSNI very regularly reviews the retention of CCTV material and deletes any data that no longer must be held.[138]

120. PSNI officers have provided numerous examples of cases to the Human Rights Advisor to illustrate the positive impact of CCTV footage and where it helped a vulnerable person or in arresting an offender. These cases range from attempted suicide or self-harm, domestic abuse, theft, assault, drug use, missing persons, rape, and attempted rape. For example, CCTV footage provided useful in arresting an offender who tracked a victim from Belfast City Centre to their home and sexually assaulted them. Police were also able to help a vulnerable person who attempted suicide in the River Lagan. Not only can CCTV help in arresting offenders but is also crucial evidence in criminal trials. PSNI data has shown that in one month, seven missing persons were found in Belfast using CCTV, and three attempted suicides were caught on CCTV, highlighting the benefits of the technology.[139]

## BODY WORN VIDEO

121. Body Worn Video (BWV) involves the use of cameras that are worn by a person and are attached onto the front of clothing or a uniform. These devices are capable of recording both visual and audio information. This type of surveillance therefore has the potential to be more intrusive than conventional CCTV systems. Scenarios could include face-to-face on doorsteps, on public transport or inside buildings such as homes and shops.[140] A body camera turns the wearer into a 'mobile surveillance system'. Therefore, at the start of any recording or as soon as practicable, the user should make a verbal announcement to indicate that the

138 A full list of the types of data and files and the retention period and corresponding review and deletion schedule can be accessed here: https://www.psni.police.uk/sites/default/files/2022-07/Police%20Service%20of%20Northern%20Ireland%20-%20Review%2C%20Retention%20and%20Disposal%20Schedule%20V0.3.pdf

139 PSNI City Centre CCTV Analytics August 2022 Report

140 https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/cctv-and-video-surveillance/guidance-on-video-surveillance-including-cctv/additional-considerations-for-technologies-other-than-cctv/

BWV equipment has been activated. This announcement should be captured on the recording. BWV used by the PSNI also has a visible red light which comes on when the camera is recording.

122. BWV can have many benefits. Recordings can provide evidence that supports grounds for an arrest.[141] In cases of domestic abuse, where victims tend to diminish impact of the incident as time passes, the initial use of BWV can be used to capture immediate emotions and reactions and strengthen the case.[142] As with other surveillance technologies, the benefits must be carefully balanced against possible rights intrusions, such as the right to privacy. BWV is subject to the same standards as set out in the Surveillance Camera Code of Practice.[143] As with CCTV footage, the Data Protection Act Principles for Law Enforcement Processing apply, for further explanation see Annex A. The NPCC has also produced national guidance on BWV, in which PSNI is recognised as a contributor.[144]

123. **PSNI's use of BWV**

The rollout of BWV started in Derry/Strabane District and Belfast City District in 2016 before being rolled out across all other Districts by March 2018. The Board reported in its 2009 Human Rights Thematic Review of Domestic Abuse Policing that the use of BWV by police, when responding to domestic abuse incidents, could contribute to an increase in the outcome rate for domestic abuse crimes as the video evidence captured at the scene could assist in the prosecution of the offender.[145] The Board's recommendation that this technology should be used by all officers responding to domestic incidents was echoed by Criminal Justice Inspectorate for Northern Ireland (CJINI) in its own 2010 thematic inspection of the handling of domestic violence and abuse cases by the criminal justice system in Northern Ireland.

124. PSNI have approximately 2,200 cameras available for officers, meaning each officer should be able to check out a camera when on shift. Following use of the camera, it is returned to the docking/charging station at which point the recordings are uploaded to the system and the camera is wiped. The uploaded recordings are then marked as evidentiary or otherwise. The camera itself is tamper proof and encryption ensures that if lost or stolen, the data would not be of

141 5 See e.g. Ngoie v R [2020] EWCA Crim 292 on the disputed role of a suspected drug dealer in the rear of the vehicle when the alleged drug deal was recorded by officers.
142 p. 29, https://library.college.police.uk/docs/NPCC/Body-worn-video-2022.pdf
143 Home Office, Surveillance Camera Code of Practice, Principle 8.1
144 https://library.college.police.uk/docs/NPCC/Body-worn-video-2022.pdf
145 NIPB, Human Rights Thematic Review, Domestic Abuse, 2009 https://www.nipolicingboard.org.uk/files/nipolicingboard/2023-01/foi-human-rights-thematic-review-domestic-abuse-march-2009.PDF

use as it must be returned to the docking station for information to be obtained.[146] BWV footage that has not been marked as evidential within the video manager system will be automatically deleted after the expiry of 31 days, and the footage cannot be recovered once deleted from this system. The video management software also has the capability to pixilate individuals' features thereby making them unidentifiable, which is necessary for use in court.[147] These policies all comply with the recommendations made by the ICO for use of BWV.[148]

125. **PSNI Policy on BWV**

The PSNI guidance on BWV states that the following are key situations in which to use BWV:

- **'Domestic abuse** incidents should be recorded. Any Domestic Abuse incidents without a recording will require a reasoned explanation why this is so, which will need to be agreed by a supervisor and noted
- **Stop and Search** encounters must be recorded in their entirety. Any Stop and Search incidents without a recording will require a reasoned explanation why this is so, which will need to be agreed by a supervisor and noted.
- **Spit and Bite Guards**: Body Worn Video must be used when applying Spit and Bite Guards outside the custody suite. Any encounters without a recording will require a reasoned explanation why this is so, which will need to be agreed by a supervisor and noted.
- **Use of Force:** Officers should use BWV to capture any incident where it is reasonably foreseeable that the use of force may be necessary. The entirety of the incident should be recorded. Any use of force encounters without a recording will require a reasoned explanation why this is so, which will need to be agreed by a supervisor.
- **Custody:** BWV must be used to record any use of force incident or any incident where it is reasonably foreseeable that the use of force may be necessary outside the custody suite. The custody suite is defined as the area inside the building which is covered by CCTV. It does not include the car park or vehicle dock. BWV must be activated by the officer/staff deploying the tactic and must remain activated for the duration of the deployment. Any Use of Force encounters without a recording will require a reasoned explanation why this is so, which will need to be agreed by a supervisor.'[149]

146 PSNI BWV Privacy Impact Assessment
147 Ibid.
148 https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/cctv-and-video-surveillance/guidance-on-video-surveillance-including-cctv/additional-considerations-for-technologies-other-than-cctv/
149 PSNI Operational Guidance: Use Of Body Worn Video (BWV)

126. The guidance also prescribes that BWV must not be used within court premises, indiscriminately for an entire encounter, during an intimate or strip search or where the recording might breach legal privilege. The Police Ombudsman investigated an incident in 2019 where a PSNI officer failed to inform a solicitor that they were filming.[150] Guidance issued in February 2023 expects supervisors to review all evidential BWV footage being exhibited and submitted to the PPS.[151] Supervisors are also expected to dip sample the following incidents: use of force, traffic stops, stop and search, domestic incidents. Additionally, supervisors are expected to view all footage from the following incidents:

- Where any force is used on a child or young person;
- Where any force is used on a vulnerable person;
- Where a Spit and Bite Guard has been used; and
- Where it is apparent that a detained person or a member of the public sustained an injury due to the Use of Force.

127. **Effects of BWV**

An investigation by the Police Ombudsman has found that there has been a 9% decrease in complaints received by the Office since the introduction of BWV by the PSNI. Complaints arising from police searches and arrests decreased the most. There had been a 10% decrease in allegations received by the Office since the introduction of BWV, such as allegations of oppressive behaviour.[152] Similar outcomes were found by reviews conducted by the College of Policing. In terms of non-crime outcomes, evidence from one of the College's reviews suggests that use of cameras can reduce complaints against officers. In terms of mechanisms, it is assumed that the process of being recorded by BWV causes a change in police officer and public behaviour, which affects the nature of the interaction between the parties. Also, BWV can provide officers with an additional level of information to assist recall when writing statements and giving evidence.[153]

128. **Confessions made on BWV**

A confession is a written or oral acknowledgment of guilt, partial involvement, knowledge or presence by a person accused of an offense – an admission contrary to the offender's interest or possible defence. Generally, evidence of an admission can be given by anyone without any particular restrictions or rules.

150 https://www.policeombudsman.org/Media-Releases/2020/Police-officer-breached-guidelines-by-failing-to-i
151 PSNI Guidance for Supervisors for reviewing and dip-sampling Body Worn Video Footage, February 2023
152 Impact of the introduction of body-worn video by the PSNI on police complaints in Northern Ireland, Police Ombudsman for Northern Ireland, 2020, https://www.policeombudsman.org/PONI/files/a8/a8019604-0930-46b3-b989-f67954421ea8.pdf
153 https://www.college.police.uk/research/crime-reduction-toolkit/body-worn-cameras

PACE Order 1989 sets out the powers and duties of the interviewer, the rights of suspects, the admissibility of evidence and therefore the protections that apply to admissions made to police officers.[154] Someone who is being interviewed by the police is 'cautioned'. All formal police interviews with suspects, whether they are there voluntarily or under arrest, start with the officer giving the suspect 'the caution' stating 'you do not have to say anything but it may harm your defence if you do not mention something when questioned that you later rely on in court. Anything you do say may be given in evidence.' [155]

129. The courts are likely to exclude an admission – such as an admission made on BWV without caution – if the protections in PACE and Code C have not been complied with – particularly:

- Access to lawyer before an interview;
- Access to medical assistance if necessary;
- Rest/sleep, food etc; and
- Good evidence of the admission (recording).

If, in a later 'PACE compliant interview,' a suspect is reminded of an admission recorded on BWV it puts them in a difficult position however.

130. Article 76 of PACE deals with challenges to the admissibility of confessions in criminal proceedings. Article 76(2) PACE directs the court to exclude confession evidence obtained by oppression; in circumstances which were likely to make the confession unreliable. Article 76(4) allows facts discovered as a result of the confession, or of the way in which defendants speak, write or express themselves, to be adduced (introduced) where relevant. This means that a statement that was not in itself admissible which led to the police obtaining other evidence is likely to be admissible. Article 78 of PACE provides a discretion for the court to exclude evidence which would otherwise be admissible against a defendant on the basis it would be unfair to adduce (introduce) it.[156]

154 This Order replicates the law in the England and Wales PACE Act 1984.

155 See Pace Code C 10.1. Code C deals with the detention, treatment and questioning of persons by police officers. https://www.justice-ni.gov.uk/sites/default/files/publications/doj/16-06-pace-code-c-2015.pdf

156 In McGuinness v The Public Prosecution Service for Northern Ireland the court dismissed an appeal by the defendant who had been convicted of assault on the basis of BWV footage. Officers responded to a call and the victim was recorded describing the alleged assault. The victim subsequently withdrew her complaint and refused to give evidence at trial.

## AIRCRAFT AND PRIVACY

131. Camera-enabled drones and helicopters can be used for:

- searching for suspects;
- searching for vulnerable missing people;
- searching for stolen property and vehicles;
- overseeing large police operations;
- getting aerial imagery of crime scenes and serious road traffic collisions; and
- assisting in planning police operations.

However, surveillance drones may also be used to remotely monitor and track people's movements in public spaces, including at protests. Police in England have used drones to monitor Black Lives Matter and Extinction Rebellion protests.[157]

132. PSNI have the use of three helicopters and two fixed wing aircraft. They now also have the use of 22 operational new Small Unmanned Aircraft, usually also known as drones. Requesting any of the aircraft goes through the same process. The drones have 30 mins endurance and high-definition cameras with heat sensitive capability. The PSNI have significant numbers of extra batteries that can ensure continued use (subject to landing for exchange). Civil Aviation Authority rules require line of sight by operator of the drone when it is use. The drones obviously need to be driven to the place where they will be launched and used. The drones are not allowed to fly over crowds, but the cameras are sufficiently powerful to use from a distance. Their main use is likely to be used for search and rescue and supporting other operations, including searching for suspects. Legislation on the use of drones both for the PSNI and members of the public is set out in the Air Navigation Order Amendment Act 2020. Each use of aerial surveillance of a particular person requires an authorisation, and the parameters of each use are included in the individual Surveillance Authority, granted under the Regulation of Investigatory Powers Act (RIPA).[158]

157 https://www.theguardian.com/uk-news/2021/feb/14/drones-police-england-monitor-political-protests-blm-extinction-rebellion, https://www.theguardian.com/world/2022/dec/05/met-police-illegally-filmed-children-as-young-as-10-at-climate-protest

158 For further legislative background on the use of drones and previous recommendations by the NIPB, please refer to Annex C.

## ANPR (AUTOMATIC NUMBER PLATE RECOGNITION)

133. In a 2016 speech the then Surveillance Camera Commissioner Tony Porter pointed out:

> 'ANPR in UK must surely be one of the largest data gatherers of its citizens in the world. Mining of meta-data – overlaying against other databases can be far more intrusive than communication intercept.'[159]

134. This means that strict controls over how this data is collected, stored, and accessed are crucial. ANPR works in the following way: As a vehicle passes an ANPR camera, the camera takes a snapshot of a vehicle's number plate and then converts that image into machine-encoded text – this is known as optical character recognition. The vehicle registration is then cross-checked with whichever database is being used by the ANPR operator for their specific requirements. ANPR technology is used by Law Enforcement Agencies (LEAs) including the police, as well as private companies, local authorities, the DVSA and the DVLA.

135. Police ANPR reads a vehicle's registration number as it passes a number plate recognition camera and is instantly checked against database records of 'vehicles of interest'. Police officers can stop a vehicle, speak to the occupants and, where necessary, make arrests. ANPR can help locate people wanted for arrest or missing, witnesses, stolen vehicles, uninsured vehicles and uncovering cases of major crime. A record for all vehicles passing by a camera is stored, including those for vehicles that are not known to be of interest at the time of the read. According to the Metropolitan Police, at present ANPR cameras submit on average around 60 million ANPR 'read' records to national ANPR systems daily.[160] ANPR data from each police force is stored together with similar data from other forces for one year.

ANPR reads can detect or be used to calculate the following:

- Average speed of vehicles;
- Untaxed vehicles;
- Uninsured vehicles;
- Stolen vehicles;

159 Surveillance Camera Commissioner's speech to the national ANPR conference, 2016, https://www.gov.uk/government/speeches/speech-to-the-national-automatic-number-plate-recognition-conference

160 https://www.met.police.uk/advice/advice-and-information/rs/road-safety/automatic-number-plate-recognition-anpr/

- Instances of terrorism, major and organised crime;
- Traffic flow;
- Bus lanes and box junctions;
- Parking in car parks;
- The use of toll roads;
- The London congestion zone; and
- Traffic journey times.

136. ANPR also reads the Vehicle Registration Mark (VRM). This is a unique mark linked to a specific vehicle, displayed on its number plate. According to the ICO, in most circumstances, a VRM is personal data. However, this can depend on the context of the processing. A VRM is personal data at the point where you collect it, if you process it as part of a surveillance system for the purposes of identifying an individual (potentially to take some action, such as to serve them with a parking fine).[161] The UK has a National Law Enforcement ANPR capability (NAC) which enables LEAs to benefit from operational use of ANPR. This includes a single national store of ANPR data and a national infrastructure of ANPR cameras, communication links, firewalls, and other components. ANPR is governed by Data Standards, Infrastructure Standards and Data Access and Management Standards, which are bundled together in the National ANPR Standards for Policing and Law Enforcement.[162] Furthermore, the Home Office has separate audit guidelines for law enforcement ANPR.[163]

137. As with CCTV technology, ANPR is subject to Part 3 of the Data Protection Act and the Surveillance Camera Code of Practice. Similar to CCTV, the National Law Enforcement ANPR capability (NAC) is subject to the Information Commissioner's Office regulatory provisions and regulatory oversight by the Biometrics and Surveillance Camera Commissioner. According to the National ANPR Standards, a Data Protection Impact Assessment (DPIA), which may include consultations with relevant stakeholders, is required for all planned new infrastructure. When a DPIA identifies a large increase in the number of deployed ANPR infrastructure or where significant privacy risks are identified the Information Commissioner's Office (ICO) should be consulted.

161 https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/cctv-and-video-surveillance/guidance-on-video-surveillance-including-cctv/additional-considerations-for-technologies-other-than-cctv/#anpr

162 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1091167/NASPLE_Version_2.4_July_2022.pdf As with CCTV, the Protection of Freedoms Act 2012 ch 2 requires a Code of Practice for ANPR.

163 National Standards for Compliance and Audit of Law Enforcement ANPR, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/913991/ANPR_Compliance_and_Audit_Standards_v2.0_September_2020.pdf

138. In his 2020/21 report, the Biometrics and Surveillance Camera Commissioner stated:

'The standards for the use of ANPR in policing and law enforcement are comprehensive and stand out as providing a robust and exemplary framework fundamental to assuring the transparent and proportionate use of ANPR technology.'[164]

According to the latest report by the Biometrics and Surveillance Camera Commissioner, ANPR systems will read 100m vehicle number plates by 2023/24, making it the largest non-military database in the UK. The vast majority of these 'reads' will have to be ignored because of the sheer volume of data, raising questions of proportionality and legitimacy.[165]

139. The Biometrics and Surveillance Camera Commissioner chairs the Independent Advisory Group on ANPR, which regularly meets.[166]

140. When Transport for London wanted to use ANPR to monitor adherence to the Ultra Low Emission Zone, the Commissioner highlighted the risk in using ANPR beyond its purpose:

'Extending the use of the role of ANPR is beyond its initial purpose and causes further concern over its legitimacy. There are ongoing issues around the lack of statutory footing for ANPR. There are also concerns around proportionality and who gets access to the data.'[167]

141. **PSNI's use of ANPR**

PSNI retains and analyses ANPR data collected in Northern Ireland and adhere to the National ANPR Standards for Policing and Law Enforcement. According to PSNI, staff only have access to ANPR data if it is relevant to their role, and the majority of those who have permission may only do so for a maximum period of 90 days from the date it was collected. Certain staff are authorised to access data older than 90 days subject to further scrutiny. After 90 days, access may only be for serious, major or counter terrorism investigations and where a senior officer has authorised access.[168]

164 p.22
165 Office of the Biometrics and Surveillance Camera Commissioner, Annual Report 2021/22, paras 139 - 140
166 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1067709/ANPR_IAG_meeting_minutes_21-03-2022_final__1_.pdf
167 https://www.gov.uk/government/publications/tfl-consultation-on-ulez-expansion-commissioner-response/commissioner-response-to-the-tfl-consultation-on-ulez-expansion
168 https://www.psni.police.uk/about-us/our-policies-and-procedures/automatic-number-plate-recognition

There are currently 234 active ANPR sites, 109 of which are permanent, in Northern Ireland,[169] which the Road Safety Partnership operates across Northern Ireland.[170] The ANPR system in Northern Ireland was designed and built by the British Army and handed over to PSNI when Operation Banner came to a close.

169 https://www.nidirect.gov.uk/articles/types-and-locations-safety-cameras

170 The Partnership includes representatives of the Department of the Environment, Department of Regional Development (Transport NI), The Police Service of Northern Ireland, The Northern Ireland Courts and Tribunal Service and the Department of Justice. See more at https://www.psni.police.uk/safety-and-support/keeping-safe/protecting-yourself/protect-yourself-when-driving/northern-ireland

# CHAPTER 6:
# TARGETED SURVEILLANCE

142. '…Powers of secret surveillance of citizens, characterising as they do the police state, are tolerable under the Convention only in so far as strictly necessary for safeguarding the democratic institutions…The Court must be satisfied that, whatever system of surveillance is adopted, there exist adequate and effective guarantees against abuse…'[171]

## SURVEILLANCE AND PRIVACY RIGHTS

143. Taking telephone tapping (targeted interception) and metering[172] as examples, the ECtHR has found violations of Article 8 in the following spheres:

- 'phone tapping and supply of records of metering to the police (list of telephone numbers called);
- monitoring and transcription of all the applicants' commercial and private phone calls; monitoring and recording of several of the applicant's phone conversations by tapping a third party's telephone line;
- telephone conversations monitored in the context of a criminal prosecution and subsequently published in the press;
- inclusion in the applicant's case file of a transcription from phone tapping carried out in proceedings in which he had not been involved;
- monitoring of phone calls by the authorities in the absence of authorisation by the public prosecutor issued in the name of the suspect and without legislation providing sufficient safeguards against arbitrariness;
- tapping of phone calls made by a lawyer for criminal investigations;
- insufficient safeguards against arbitrariness in domestic provisions on phone tapping;
- unjustified failure to provide *ex post* notification of a temporary mobile phone tapping measure;
- preventive monitoring of phone calls;
- the practically unlimited power of the intelligence services in carrying out surveillance of an individual and of meetings held in the flat that he owned without sufficient legal safeguards, which also randomly affected another person without any protection being provided under domestic law for such a person; and

171 Paras 42 & 50, Klass and Others v Germany.
172 Metering' involves using a device to register the numbers dialed on a telephone, the time and duration of each call.

- the interception, recording and transcription of a telephone conversation between a lawyer and one of his clients, a former defence minister, who was under covert surveillance in connection with a criminal investigation.'[173]

## UK LEGISLATION

144. Covert surveillance powers are governed by the Police Act 1997 (PA), the Regulation of Investigatory Powers Act 2000 (RIPA), the Investigatory Powers Act 2016 (IPA) and the many other formal and statutory codes.[174] All these provisions apply directly in Northern Ireland to the PSNI and the other law enforcement bodies working in Northern Ireland. These provisions include the following powers and procedures for the police service:

- the interception of communications (in the course of its transmission by means of a public postal service or public or private telecommunication system) (including 'telephone tapping' – listening in to a person's telephone calls);
- intrusive surveillance on residential premises and in private vehicles (use of listening devices);
- covert access to homes and properties (searching homes or installing cameras or surveillance devices);
- covert (directed against a particular person) surveillance;
- the use of Covert Human Intelligence Sources (CHIS - commonly referred to as police informants, agents or undercover officers[175]);
- the authorisation of criminal conduct by those informants, agents or undercover officers (Criminal Conduct Authorisations);
- the acquisition of communications data (for example itemised telephone billing, telephone subscriber details and internet visiting data);
- Equipment interference (obtaining information from computers and other devices); and
- the investigation of electronic data protected by encryption (requiring a person to disclose their passwords).

145. The current legislation was introduced piecemeal (and often as a result of human rights litigation) in 1985, 1989, 1994, 1997 and then importantly in 2000, in parallel with the Human Rights Act.[176] Further legislation was introduced in 2016 and 2021.

173 Para 127, Guide to the Caselaw of the European Court of Human Rights, Data Protection, August 2022. Case references removed.

174 Including, for instance, the Covert Surveillance and Property Interference, Revised Code of Practice, August 2018.

175 'What does anonymity ruling mean for undercover police?', the Detail, 7 November 2012.

176 Covert Human Intelligence Sources and Authorising Crime, John Wadham, European Human Rights Law Review, 2021, Issue 4.

The most important change was set out in the Regulation of Investigatory Powers Act 2000 which was designed to ensure that the procedures complied with the principles already set out by the ECtHR under Article 8. Before all these provisions existed the procedure used by police officers to listen in to telephone calls or to place listening devices in homes, offices and cars was only set out in internal, and often secret, guidance.[177] The improvements in regulation and transparency only came about by NGOs and others taking cases to courts (particularly the ECtHR).[178]

The PA, RIPA and the IPA provisions require the following techniques, used by PSNI, to be regulated:

146. **Telephone interception**

Listening in to a person's telephone calls without consent is considered by the law to be a very serious invasion of privacy and, therefore, it is a criminal offence to intercept telephone communications without a warrant.[179] Warrants can only be granted by a Secretary of State on the basis of national security, preventing or detecting serious crime or in the interests of the economic well-being of the UK.[180] The Chief Constable of the PSNI, unlike most other forces in the UK can apply directly to the Secretary of State for a targeted interception warrant. There are some enhanced protections for the telephone calls of Members of Parliament, journalists, and for privileged communications between lawyers and clients.[181] There are also strict rules on who can have access to the content of the communication once an interception warrant is in place (including a prohibition on using the material produced in courts). The Interception of Communications Code of Practice provides considerable detail on the procedures.[182]

147. **Communications data**

Access to data by police officers on the details of calls, emails, texts etc. or internet connection data[183], but not the content of the communications, is less strictly controlled. Communications data will, for instance, include the time, date,

177 Malone v UK.

178 The law is now very complicated but useful guides include: Covert Investigation, 5th ed, Clive Hartfield and Karen Harfield, Blackstone's Practical Policing; Covert Policing, Simon McKay, OUP; and the Blackstone's Guide to the Investigatory Powers Act 2016, Simon McKay, OUP. See also the Codes of Practice issued by the Home Office https://www.gov.uk/government/collections/ripa-codes

179 Strangely, the use of a listening device is person's home is not an equivalent criminal offence.

180 'Bulk warrants' are used by GCHQ, MI5 and MI6, restricted to overseas communications and have to be authorised by a Secretary of State.

181 Similar enhanced protections apply in relation to the other powers.

182 Interception of Communications Code of Practice, pursuant to Schedule 7 to the Investigatory Powers Act 2016 December 2022.

183 There are some additional restrictions that apply to this, IPA section 62.

and people called (or texted) but not a recording of the actual call, text, or material communicated. Accessing the contents of the call, text, or material communicated have considerably greater safeguards. The grounds for accessing only the communications data are much wider, including national security, preventing or detecting crime (not just serious crime), public safety or health, and preventing disorder.[184] The Office for Communications Data Authorisations (OCDA) was established following the Investigatory Powers Act (IPA) 2016 and considers requests for communications data from law enforcement and public authorities. The Investigatory Powers Commissioner (currently Sir Brian Leveson) is the head of OCDA and delegates his powers to authorise communications data requests to OCDA Authorising Officers.[185] Authorisation can also be granted by designated police inspectors in Northern Ireland.[186]

148. **Equipment interference**

The IPA also allows police officers, including the PSNI, to engage in 'equipment interference' or interference with computers and other devices in order to obtain information.[187]

149. **Directed surveillance**

Authorisation is required before police officers monitor, listen to conversations or observe or track the movement or activities of a particular person, including by recording such activities or by using a surveillance device. The justification required is similar to the test set out for communication data above and includes preventing or detecting crime or preventing disorder.[188] Authorisation can be by a Superintendent. Directed surveillance of an individual in the social media world also requires an authorisation.

150. Surveillance as part of a police officer's normal duties does not require such authorisation. So, for instance, if officers notice people acting suspiciously and, in order to maintain a view of them without raising their suspicions, they conceal themselves behind a wall no authorisation is required.[189]

151. The use of overt CCTV cameras does not normally require authorisation under RIPA or the IPA but guidance is provided in England and Wales by the Surveillance Camera Code of Practice and overseen by the Commissioner.[190]

184 IPA section 61 onwards. Internet and communications service providers are obliged to retain data for one year, IPA section 87.
185 https://www.gov.uk/government/organisations/office-for-communications-data-authorisations/about
186 See IPA Schedules 4 and 6.
187 Approval requiring a warrant from a chief officer, IPA, Part 5.
188 RIPA, section 28.
189 Page 96, Covert Investigation, 5th Ed. Harfield and Harfield.
190 Protection of Freedoms Act 2012.

However, where overt CCTV or ANPR 'are used in a covert and pre-planned manner as part of a specific investigation or operation, for the surveillance of a specific person or group of people, a directed surveillance should be considered.'[191] If there are concerns about the trustworthiness of an overt public space surveillance system (for example concerns about the use of Chinese-manufactured technology), there may be limitations on the extent to which that same technology can be trusted for use in sensitive covert operations.

152. As an example of the use of ANPR, this directed surveillance by PSNI involved suspects using a car to travel to the Republic of Ireland, source controlled drugs and bring those drugs back into Northern Ireland to be sold on. The operation involved a Directed Surveillance authority being granted which focused on the live alert of a vehicle on the ANPR system to monitor the movements of the suspect's vehicle. This would indicate when the subjects' vehicle crossed into the Republic of Ireland allowing the PSNI to stop the vehicle if and when it returned to Northern Ireland. In this case the Directed Surveillance authority allowed for the safe stop of the vehicle and the subsequent search of it, and the occupants. The searches resulted in the seizure of a quantity of class A drugs (heroin) destined for onward supply into the Northern Ireland community, and an amount of cash. Two arrests were made and the people were subsequently prosecuted for a number of offences involving controlled drugs and traffic offences. After the safe stop and search of the vehicle and occupants, the authority was cancelled.

153. **Intrusive surveillance**

Intrusive surveillance is surveillance that occurs in a private dwelling or vehicle – for instance – installing a listening device or camera. There is a higher test for this authorisation – it must be justified on the basis of preventing or detecting a **serious** crime.[192] Authorisation must be by a chief officer and is subject to prior approval by a Judicial Commissioner.

154. **Interference with property and entry on to land**

Generally, police officers must obtain a separate authorisation to enter someone's property without their consent.[193] This includes to interfere with property for the purposes of installing recording and surveillance devices.[194]

191 Para 3.39, Covert Surveillance and Property Interference, Code of Practice, 2018.
192 A serious crime is defined as one which, on first conviction for a person who has reached the age of 21, could reasonably be expected to receive three years imprisonment or involves violence, substantial financial gain or a large number of people in pursuit of a common purpose, RIPA section 81.
193 Police Act 1997, Part III.
194 Covert Surveillance and Property Interference, Code of Practice, Home Office, 2018.

155. **Social media**

A lot of information of people's lives can be gleaned from social media posts. Those posting online do so with the knowledge that it is public. Therefore, the Covert Surveillance and Property Interference Code of Practice states:

'3.10… Much of it can be accessed without the need for RIPA authorisation; use of the internet prior to an investigation should not normally engage privacy considerations. But if the study of an individual's online presence becomes persistent, or where material obtained from any check is to be extracted and recorded and may engage privacy considerations, RIPA authorisations may need to be considered. The following guidance is intended to assist public authorities in identifying when such authorisations may be appropriate.

3.11 The internet may be used for intelligence gathering and/or as a surveillance tool. Where online monitoring or investigation is conducted covertly for the purpose of a specific investigation or operation and is likely to result in the obtaining of private information about a person or group, an authorisation for directed surveillance should be considered, as set out elsewhere in this code. Where a person acting on behalf of a public authority is intending to engage with others online without disclosing his or her identity, a CHIS authorisation may be needed (paragraphs 4.10 to 4.16 of the Covert Human Intelligence Sources code of practice provide detail on where a CHIS authorisation may be available for online activity).

3.12 In deciding whether online surveillance should be regarded as covert, consideration should be given to the likelihood of the subject(s) knowing that the surveillance is or may be taking place. Use of the internet itself may be considered as adopting a surveillance technique calculated to ensure that the subject is unaware of it, even if no further steps are taken to conceal the activity. Conversely, where a public authority has taken reasonable steps to inform the public or particular individuals that the surveillance is or may be taking place, the activity may be regarded as overt and a directed surveillance authorisation will not normally be available.'[195]

156. The Human Rights Annual Report for 2020/21 recommended:

'The PSNI publish its policy on its monitoring of social media for policing purposes and include in this its retention and access arrangements. If a new policy is to be developed this should be subject to public consultation and an equality impact assessment.'

195 Covert Surveillance and Property Interference**,** Revised Code of Practice, August 2018.

157. The PSNI responded on 06/05/22:

> 'There is currently no Police Service policy that encompasses all circumstances in which personnel may access social media across all organisational areas. This is because different teams access social media for different reasons Examples include community engagement work carried out by Neighbourhood Policing teams and Senior Management teams, media monitoring by Corporate Communications, or the collection of evidence or intelligence for the purpose of the prevention or detection of crime and the prevention of disorder. When accessed for crime and disorder purposes social media can be used to efficiently obtain information that would otherwise require more intrusive and resource intensive tactics. Guidance exists advising whether activity may require authorisation under appropriate legislation. Any novel techniques may be considered in advance with a PSNI Legal Advisor and the Investigatory Powers Commissioner's Office (IPCO). Training is provided to personnel who engage in this activity. This includes how to lawfully manage any information collected. Bulk data collection techniques are not used. PSNI is subject to regular inspections by the Investigatory Powers Commissioner's Office (IPCO) who hold us accountable on behalf of the public. IPCO are currently focusing all agencies attention on the subject of data retention. This concerns arrangements that ensure data is held securely, is only accessed by people who have a genuine need, and the necessity to retain it is regularly reviewed. Members of the public also have the right to complain to the Investigatory Powers Tribunal (IPT) if they suspect PSNI have unlawfully used covert capabilities.'[196]

## COVERT HUMAN INTELLIGENCE SOURCES (CHIS)

158. A 'CHIS' is a person who collects information from his or her contacts and interactions with others and covertly passes this on to a law enforcement agency. Often known as an informant but police officers and others can also perform the role of a CHIS if they go 'undercover'. Since the discovery of some very problematic and unlawful practices by undercover officers in England and Wales new advice has been provided by the College of Policing[197] pending the final report from the Undercover Policing Inquiry.[198] Undercover policing units should be accredited.[199]

196 PSNI Letter to the NIPB
197 Undercover policing**,** Authorised Professional Practice, February 2021 v2.
198 https://www.ucpi.org.uk
199 All units that manage undercover operations should undertake a self-assessment process for accreditation to deploy undercover operatives. Units may request accreditation under three categories: foundation, advanced, and undercover online.

159. Sometimes CHIS are paid, can claim expenses, or the law enforcement agency might indicate that it is unlikely to be in the public interest to prosecute their criminality but sometimes they are solely motivated by concerns to protect victims of crime or to expose serious wrongdoing. The police use of a CHIS must be authorised in advance in accordance with RIPA. Recent legislation has allowed the PSNI not merely to authorise a CHIS but to give them (and the officer authorising it) special immunity from criminal prosecution if the criminal conduct will progress the investigation that the CHIS is already authorised.[200] However, If a CHIS commits a crime outside a Criminal Conduct Authorisation (CCA) there will be no immunity from prosecution (although both the law enforcement agency and the prosecutor will still need to assess whether a prosecution is in the public interest).

160. An example provided by PSNI was that of a CHIS who was approached by an organised crime gang to conspire with them by providing limited logistical support to their on-going criminality. The PSNI concluded that it was obvious that if the CHIS declined to assist the activity would be undertaken by another third party anyway. This would leave PSNI investigators unsighted and unable to best respond to the more serious criminality. The CHIS did so following a Criminal Conduct Authority which resulted in the seizure of criminal assets and arrests. The authority was cancelled immediately following police action.

161. The Human Rights Advisor has considered the use of CHIS by the PSNI and extracts of his last Human Rights Annual Report for 21/22 can be found in Annex E. Annex F contains an extract on PSNI's internal guidance. The Human Rights Advisor has also asked to attend an individual CHIS governance meeting to understand how one of the safeguards works in practice but this has not yet taken place.

### 162. Undercover police officers

Undercover tactics are delivered by the Covert Policing Team (CPT) who are situated within Crime Operations Department of PSNI. This is a nationally accredited team who are specifically trained. The use of undercover police officers can be a highly intrusive tactic there are both internal and external accountability mechanisms in place and the Human Rights Advisor was told that the tactic is only utilised in the following circumstances:

200 Covert Human Intelligence Sources (Criminal Conduct) Act 2021.

- After balancing the intrusive nature of the tactic against the seriousness of the offence and the harm caused to the community, the level of the intrusion, and any potential of involvement in criminal participation.
- After appropriate application of the relevant primary legislation and case law.
- When the serious crime threshold is met and in furtherance of policing priorities.
- Following consultation with senior lawyers at the PPS.

163. Undercover operations are authorised at a minimum rank of Assistant Chief Constable and the following areas must be considered in any request for authorisation of undercover officers:

- Necessity criteria – purpose of deployment and criminality under investigation
- Operational overview and proposed operational delivery
- Proportionality considerations
- Risk assessment
- Subject(s) of the intrusion
- Collateral intrusion considerations and measures taken to mitigate
- Use and conduct sought for undercover operative

This process is largely replicated for any request for authorisation of undercover officers to engage in any criminal conduct. Undercover officers are trained before embarking on their work and the Human Rights Advisor was invited to attend the next training session.

164. In Northern Ireland, there appears to be no evidence of the kind of problems that existed in England and Wales some time ago. Recently Counsel to the Undercover Policing Inquiry said:

'The whole operation was secret and a very high priority was accorded to keeping it that way. Courts were sometimes misled. Miscarriages of justice occurred as a result. An officer whose cover was compromised was told to pretend that he was acting independently. Discipline was not enforced. Aspects of deceased's children's identities were used even though they added only a limited further protection.

These operations have caused a lot of harm. Democratic freedoms have been infringed, outrage and pain has been caused. The damage is not limited to members of the public. Former undercover officers have suffered psychiatric injury.

The primary reason for conducting these operations was to gain intelligence to assist police to maintain order on the streets. However, the level of threat posed to public order was often not commensurate with a need to deploy undercover police officers for this purpose. Not in the way that they operated. The benefits which the unit's intelligence brought to public order policing do not, in our submission, justify the means.' [201]

165. Governance is much more significant now and the CPT are subject to an annual inspection by the Investigatory Powers Commissioners Office (IPCO). These inspections are conducted to assess compliance with RIPA 2000 and the relevant Codes of Practice, with a particular focus on the authorisation process and recordkeeping. The CPT is accredited by the College of Policing to deliver undercover policing operations as well as internal training.[202] This is an accreditation process which focuses on the personnel and systems required to deliver the tactic. The CPT also participate in the NPCC National Undercover Working Group who are responsible for issuing guidance and direction to undercover units, including the development of standardised procedures, consistency of training and the welfare of officers.

166. Standards and culture commence at the recruitment of officers into the undercover role and all officers are regularly reminded that their reputation and integrity is critical to confidence in policing. In addition, there is a national Code of Conduct for undercover operatives which reinforces personal responsibilities. At every operational briefing a set of instructions are read to undercover officers. These instructions cover critical areas such as not acting as an agent provocateur, doing no more than offering an unexceptional opportunity to a person to commit crime and ensuring their involvement is any operation in their undercover role is authorised. There is a need to balance exposure of the tactic to preserve its operational effectiveness to protect the vulnerable from harm. The wellbeing and welfare of officers involved in undercover policing is also a significant consideration.

167. The Human Rights Advisor discussed several examples with CPT and authorisation paperwork was available to view. The Human Rights Advisor was shown several authorisations which also involved a separate Criminal Conduct Authorisation. These included the use of undercover officers in a passive manner

201 Closing Statement for Tranche 1, 16th February 2023

202 Authorised Professional Practice: Undercover Policing, College of Policing, February 2021. Interestingly the words 'human rights' do not appear in the text. However, the principles, particularly those derived from article 8, the right to privacy form the basis of the Regulation of Investigatory Powers Act and those are therefore, the bedrock of much of the text in this publication.

to identify and arrest those involved in child sexual exploitation and abuse online, drugs supply fuelling drug deaths, human trafficking offences and suspects attempting to procure firearms on the darkweb. Authorisations have to be by an Assistant Chief Constable and by the Chief himself if the operation lasts for more than nine months. Examples of successful undercover operations include:

- An undercover operative deployed online as a 13-year-old girl. A username engaged the child profile in a highly sexualised conversation and indicated his desire to meet for sex. Four days later the male travelled to meet the 13-year-old profile in Belfast and was arrested. He was identified as a 39-year-old male and a father of 4 young children. He subsequently pleaded guilty to a number of child sexual offences and his sentencing hearing was the subject of media reporting. He received 1 year imprisonment and 2 years on licence, 10-year SOPO and Sex Offender Registration.
- As a response to the sharp increase in drugs deaths in NI operatives deployed online to identify those anonymous usernames involved in the sale of illicit drugs. An undercover operative deployed and bought prescription medications. The suspect was identified and was arrested in possession of approximately 1000 tablets. During a follow up search 20,000 tablets were seized plus thousands of empty boxes which had already been sold. The suspect was charged with various drugs offences.
- A male attempted to procure a Glock handgun, ammunitions and a silencer on the dark web. An operative engaged the suspect as a firearms vendor and met with the suspect for the sale. The suspect was identified as a then serving PSNI officer. The suspect was given an 11 year custodial sentence.

## THE ROLE OF COMMISSIONERS IN RELATION TO COVERT SURVEILLANCE

168. The IPA created in 2016 a new role – the Investigatory Powers Commissioner and, with it, a number of judicial commissioners. The Commissioner and the judicial commissioners are appointed by the Prime Minister. Under the statute, Judicial Commissioners need to hold or have held high judicial office i.e. the High Court or above. There was to be an Investigatory Powers Commissioner specifically for Northern Ireland, but that role has never been filled as previously mentioned. The job of the commissioners is to consider whether authorisations or warrant applications made by the Public Authorities (such as a law enforcement agency) themselves were properly and lawfully made. Judicial Commissioners act as an independent safeguard to the primary decisionmaker and will review necessity and proportionality and have regard to privacy considerations.[203]

203 See para 19 of the Advisory Notice 1/2018 https://ipco-wpmedia-prod-s3.s3.eu-west-2.amazonaws.com/20180403-IPCO-Guidance-Note-2.pdf

In particular:

- whether what is sought to be achieved by the warrant, authorisation or notice could reasonably be achieved by other less intrusive means;
- whether the level of protection to be applied in relation to any obtaining of information by virtue of the warrant, authorisation or notice is higher because of the particular sensitivity of that information;
- the public interest in the integrity and security of telecommunication systems and postal services; and
- any other aspects of the public interest in the protection of privacy.[204]

169. One of the other key roles of the Investigatory Powers Commissioner's Office (IPCO) is to inspect the procedures and processes of all the institutions that authorise and use surveillance powers and to inspect the exercise of these powers. Each year the Office inspects the activities of PSNI and provides the PSNI with a detailed report. IPCO also have a function in relation to error reporting.[205] IPCO also now has guidance for whistle-blowers who wish to report unlawful use of investigatory powers.[206] Finally IPCO is likely to inherit the work of the Biometric Commissioner as proposed in the Data Protection and Digital Identity Bill which is currently being considered by the UK Parliament.[207]

170. For the year 2020 the IPCO summarised its report on the PSNI as follows:

'14.65 In general, PSNI demonstrated a good level of compliance with the IPA and its associated Code of Practice. Necessity and proportionality cases were well made and clearly set out. We saw good use of thematic warrants and timely modifications as required. However, PSNI has an IPA compliance risk in relation to the safeguards governing how IPA and RIPA material should be handled. Two areas of risk were identified by PSNI and reported to us, in relation to warranted data from two different sources: both relate to the retention of IPA and RIPA material beyond the time that is necessary for the authorised purpose (in fact PSNI was retaining the material indefinitely).

14.66 These areas are now subject to mitigation and extra oversight. In 2020, we wrote to PSNI advising it should introduce a RRD process for TI product at the earliest opportunity. PSNI has been working to address these issues and has

204 Ibid. para 16
205 https://www.ipco.org.uk/what-we-do/errors/
206 Disclosing information to IPCO: Guidance for those who want to disclose information about the use of investigatory Powers, August 2022.
207 https://bills.parliament.uk/bills/3430

indicated that new processes are in place in relation to retention and deletion; these will satisfy the requirements of the IPA safeguards for both these sets of data. We are returning for an IPA safeguards inspection in early 2021 to check compliance.'[208]

And for 2021:

'13.55 Overall, we were satisfied that PSNI had achieved a high level of compliance with the IPA. We examined a number of applications, renewals and cancellations and were satisfied that necessity and proportionality considerations were properly being articulated. We saw good examples of assessments of collateral intrusion.

13.56 We examined whether the appropriate amount of detail was being included in minor and major modifications which are not subject to prior approval by Judicial Commissioners. We were satisfied that modifications were being used appropriately and provided the necessary operational flexibility foreseen by the Act. In our view, the modifications fell within the foreseeable scope of the application and renewal documentation set out the scale and scope of operations clearly. We also saw good early use of modifications to remove factors that were no longer deemed necessary.

13.57 PSNI has resolved the two compliance matters we referred to in our 2020 report and which related to the retention of IPA data. We have been in correspondence throughout the year, have inspected the areas concerned and we are satisfied that PSNI is now fully compliant…

17.8 We were satisfied that the NIO is discharging its function as a gateway for advice to the Secretary of State to a very high standard. Officials carefully examine submissions, the vast majority of which are from MI5 and Police Service of Northern Ireland (PSNI), challenging them where appropriate and producing objective and balanced advice for the Secretary of State. We identified some good practice during the inspection, particularly the processes developed for keeping intercepting agency handling arrangements under review.'[209]

171. The Human Rights Advisor has reviewed the specific inspection reports by the IPCO over the last few years and noted that, overall, it is positive in respect of PSNI practice and procedure. An extract of the latest report can be found in Annex D.

208 IPCO Annual Report for 2020.
209 Report for 2021, March 2023.

The Human Rights Annual Report 2020/21 recommended that these reports should be published (suitably redacted). The PSNI did not accept the recommendation and responded:

'The PSNI provides full access for the Human Rights Advisor to the annual inspection reports together with a full briefing regarding the Service action plan in respect of any observations or recommendation which have been made. Given the operational sensitivities and very detailed covert methodology contained in these reports there is a risk to covert tactics and capability if this material exposed and, therefore, it is not feasible to publish the reports even in a redacted or summary form.

The PSNI is committed to continuing the current arrangement whereby NIPB Human Rights Advisor has access to all relevant Regulation of Investigatory Powers Act and Investigatory Powers Act material to review so that they can appraise the Board of human rights compliance. Furthermore, RIPA and IPA Codes of Practice which guide the Police Service in its approach to covert tactics and which form the basis of our internal policies and guidance is publicly available.'[210]

The Human Rights Advisor was grateful to the PSNI and to the Investigatory Powers Commissioner, Sir Brian Leveson, to be given the opportunity of being present in May 2023 when, immediately after the IPCO annual inspection of the PSNI, the inspectors and one of the Commissioners provided their initial findings to senior PSNI officers. It is hoped that, once IPCO's written report has been provided to PSNI, further details can be included in the Human Rights Advisor's next report. This appears to be the first time that a third party has been allowed to attend the inspection in Northern Ireland. It is also understood that requests by Police and Crime Commissioners to attend similar IPCO inspectors' end of inspection sessions in England and Wales have, apparently, been refused. Perhaps, an important reason for having 'Developed Vetted' Human Rights Advisor working for the Policing Board.

210 See recent reference to the possibility of disclosure after checking with IPCO, IPCO Quarterly Newsletter, Winter 2022.

## INVESTIGATORY POWERS TRIBUNAL

172. The Investigatory Powers Tribunal (IPT) deals with complaints from individuals who believe that they were subject to some kind of unlawful surveillance or there was a breach of the Human Rights Act as a result of the use of these powers.[211] There are, in fact, very few credible complaints to the IPT, because few people know about its existence but, not least because the secret nature of surveillance means that few people know it is happening and, even fewer, have any evidence that it was carried out improperly.[212] Despite these obstacles, credible cases have included: human rights NGOs;[213] several police officers subject to surveillance by their own forces investigating misconduct;[214] journalists;[215] cases relating to the police requiring a person to supply the PIN number for a phone;[216] and the use of undercover police officers. One well publicised recent case concerning Metropolitan Police undercover officers revealed:

173. 'From 2003 to 2009, a police operation was in place to collect intelligence about public disorder by political activists. The focus was on public disorder that amounted to or involved criminal acts but inevitably also collected intelligence concerning legitimate and lawful public protest…

174. Within months of starting his deployment, Kennedy (a married man with children) had entered into an intimate sexual relationship with … the Claimant, which lasted until 2005. During that time he insinuated himself into every aspect of her private and family life. Thereafter Kennedy entered into sexual relationships with other women under surveillance, as did a number of other undercover police officers engaged in similar work.'[217] As a result of the case the claimant was awarded £225,971.96 in compensation.

211 https://www.ipt-uk.com See also the on this website speech by the Chair of the IPT Sir Rabinder Singh, 'Holding the Balance: National Security, Civil Liberties and the Role of the Investigatory Powers Tribunal', 20 February 2019.
212 In both 2020 and 2021 the Tribunal did not rule in favour of any complainant, page 23, Investigatory Powers Tribunal Report 2016-2021.
213 The Third Direction Case, see below.
214 For instance, Sally Bartram and Stephen Howe v The Chief Constable of The British Transport Police, IPT/19/181/CH & IPT/20/31/CH; and Gary Davies v British Transport Police, IPT 17/93/H.
215 Wilkinson and Humphries v the Chief Constable of Cleveland Police, IPT/17/84/H and IPT/17/85/H.
216 CLS v Commissioner of Police for the Metropolis, IPT/20/89/CH.
217 Wilson v (1) Commissioner of Police of The Metropolis (2) National Police Chiefs' Council, IPT/11/167/H. See also the current Under Cover Policing Inquiry, https://www.ucpi.org.uk.

## IPT CASE AGAINST THE PSNI

175. Most of the cases dealt with by the IPT do not result in a public hearing or a published judgment and there appears to be no published judgment involving the PSNI. It is understood that the first case against the PSNI in the Tribunal was heard in May 2022, some parts of which were discussed in the media.[218] The media at the time reported that the Tribunal was considering complaints made by two former senior police officers. The complaints concerned the way that they were investigated by the PSNI during an anti-corruption inquiry.[219] The media reported that the case concerned an investigation in 2014 into bribery and misconduct in public office in relation to the vehicles supply contract – no charges were brought against anyone and those involved in the Tribunal case denied any wrongdoing. This case was then examined in greater detail by the BBC Spotlight programme which was shown on 16th May 2023. The Policing Board and its Human Rights Advisor are now considering the issues in this case in more detail.

## PSNI TRANSPARENCY

176. There is very little publicly available information on how the PSNI makes use of its covert powers.[220] This is despite that fact that many other public bodies make public their policy and procedures, IPCO publishes a detailed annual report every year (with up to 182 pages describing its work) and there are a considerable number of IPT judgments that are published. However, the Human Rights Advisor has met with a number of senior officers in PSNI and has been able to consider the authorisation processes for a number of different tactics. All those officers have been helpful, open and shown him everything he asked to see.

177. The Human Rights Advisor considered two specific authorisations for the use of CHIS (informants) and was shown the completed forms for those authorisations. The application for an authorisation rehearses all the other possible investigative options as part of the proportionality assessment and designed to avoid the more intrusive use of a CHIS. The authorisation appears both rigorous and thorough. The authorisation form requires the completion of sections on possible collateral privacy intrusion and proportionality. There is clear 'tasking' by investigators and limits on the data to be sought or collected.

218 At the time of writing the Board was informed about a second case pending in the IPT where the PSNI is the respondent. This case relates to allegations made about unlawful data collection in 2013. The Human Rights Advisor is seeking more information about this case from PSNI.

219 Independent, 10 May 2022; Belfast Telegraph, 10 May 2022;

220 There appears to be only one document available, Covert Surveillance of Legal Consultations, SI0117. However there is also an FOI request - Covert Human Intelligence Sources in Protest Movements which provides very little information.

178. The CHIS 'handler' produces the application which then goes to the 'controller' and finally to Authorising Officer (a Superintendent). The role of the handler is to have day to day interactions with the CHIS but there are usually at least two handlers in a meeting with a CHIS and sometimes three. Handlers are usually constables selected for their particular skills and abilities – the work always requires a focus on the welfare and safety issues of the CHIS. Sergeants will often deal with more difficult cases. Each handler deals with around five CHIS, a controller might deal with twenty CHIS and their respective handlers. Obviously, some cases will also be considered or reported to the Assistant Chief Constable, all are reviewed by IPCO. CCAs go to ACC.

179. One of these CHIS authorisations also had a separate CCA which was equally thorough and rigorous. The Human Rights Advisor was also taken through a directed surveillance example using the ANPR to system to track a known heroin dealer's journey. Finally, he was shown a property interference authorisation – tracking device placed on car of person involved in illegal activity.

### 180. Statistics

The Human Rights Advisor was shown figures on the number of authorisations for these three procedures – all were in their hundreds – with a total less of less than one thousand. The Human Rights Advisor was told that similar numbers of authorisations had occurred since 2015. PSNI officers were reluctant for the Human Rights Advisor to publish any further details of the number of authorisations.

181. PSNI – alongside other police services – do not reveal the numbers of authorisations that are made in relation to any of its covert powers although those figures are collated, supplied to the Investigatory Powers Commissioner's Office and the UK wide figures are published in the IPCO annual report.[221]

182. These UK figures included the following authorisations:

| | |
|---|---|
| **CHIS** | **2,860** |
| **Directed surveillance** | **6,847** |
| **Intrusive surveillance** | **489** |
| **Property interference** | **1,033** |
| **Communications data** | **284,953** |
| **Targeted warrants** | **3,630** |
| **Targeted equipment interference** | **3,167** |

221 Investigatory Powers Commissioner's Annual Report 2021/22, Table 19.2, https://ipco-wpmedia-prod-s3.s3.eu-west-2.amazonaws.com/Annual-Report-2021.pdf

# CHAPTER 7:
# DATA EXTRACTION FROM DIGITAL DEVICES

183. These days our whole lives are on our phones, our car logs our GPS coordinates and Alexa and Google Home have become our personal assistants. Our lives leave digital traces everywhere, and the devices we use hold information on our lives that didn't even exist twenty years ago. This new wealth of information is both a challenge and opportunity for policing and poses new challenges to the regulation of intrusive policing powers.

184. The Information Commissioner's Office (ICO) is the UK's data protection regulator. In April 2018, following Privacy International's 'Digital Stop and Search Report'[222] and the organisation's complaint to the ICO in relation to the use of MPE technology by police forces.[223] The ICO completed a UK-wide investigation into the practice of mobile phone extraction (MPE) that police use in criminal investigations, including an assessment of compliance with data protection legislation and recommendations. The ICO published three reports in 2020/21 regarding MPE in England and Wales, Scotland, and Northern Ireland[224].

185. The first report on MPE in England and Wales, along with the 2020 Court of Appeal judgment[225] began the work to reform how police forces consider the extent to which they need to obtain digital data from mobile phones[226]. The significant risks associated with highly intrusive processing of intimate data from mobile phones are now widely accepted. Consequently, police forces should only do this type of processing after considering other, more privacy-friendly, means of achieving the same investigative objective. In data protection legislation, this means that police forces must demonstrate strict necessity (with other associated conditions) for such processing to be lawful.

222 https://privacyinternational.org/sites/default/files/201803/Digital%20Stop%20and%20Search%20Report.pdf
223 https://privacyinternational.org/sites/default/files/2018-04/Complaint%20to%20ICO%20about%20Mobile%20Phone%20Extraction%2026th%20April%202018.pdf
224 Due to the Covid-19 pandemic restrictions, the ICO team was unable to directly observe the use of MPE in live investigations in Northern Ireland. The report therefore relied on policy statements and other documentation by PSNI and notes taken during engagement with officers and operational staff.
225 Bater-James and another v R (2020) EWCA Crim 790
226 https://ico.org.uk/media/about-the-ico/documents/2617838/ico-report-on-mpe-in-england-and-wales-v1_1.pdf

186. A comprehensive examination of the legislation governing mobile phone extraction, among them the Police, Crime, Sentencing, and Courts Act 2022, data protection legislation, and the Bater-James and Sultan Mohammed Judgment can be found in Annex G.

## MOBILE PHONE EXTRACTION

187. A substantial body of material relating to finances, relationships, intimate feelings, and many other areas builds up on the device and is available for scrutiny when extracted or otherwise examined. The data a device contains does not just relate to the device's owner; it often has personal data relating to many other people. These 'third parties' have the same rights under privacy and data protection legislation as those directly involved in the investigation. Their data may be as simple as basic contact details (eg one or more telephone numbers or email addresses). However, it may also relate to what they may reasonably believe were private, possibly intimate, communications with the device's user. Amongst other things, these may be:

- text messages;
- images;
- audio files; or
- videos.

188. Another important characteristic of a mobile phone is that it is often generating and storing data of its own volition, without the knowledge of its user. Data such as:

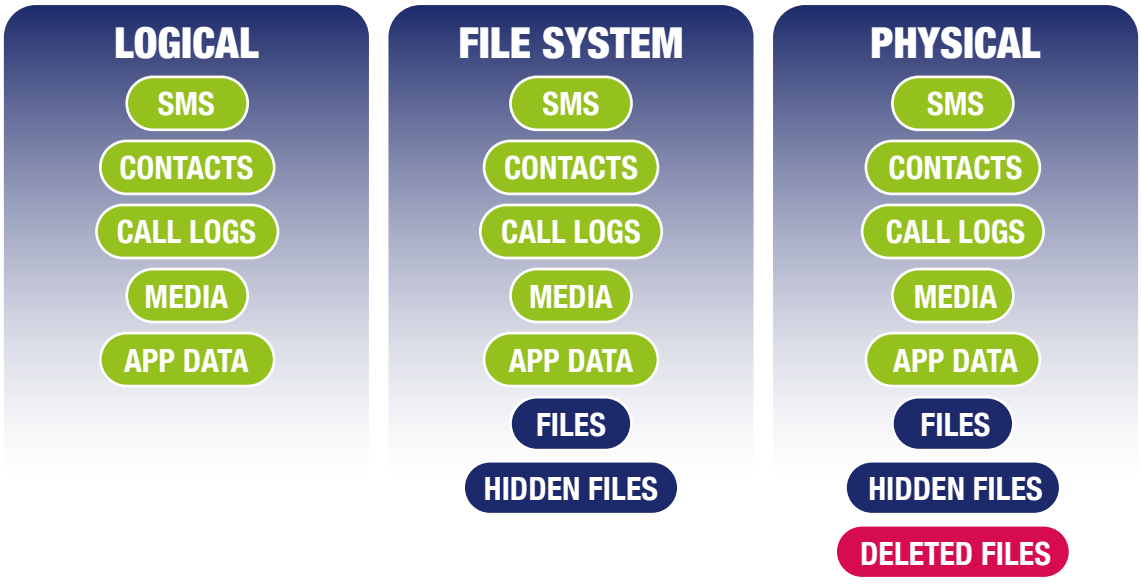
- location history;
- browsing history;
- cookies; and
- usage of apps is often being generated but is not readily visible to the user.

189. Whilst there are a range of similar 'analogue' situations where the police seek personal information from complainants and witnesses, the mobile phone is unique as a repository of data with different implications for data protection and privacy. When messaging apps such as WhatsApp are used, it is common for a sender's personal data (photos, videos or other personal information) to be placed onto the recipient's device, without the recipient's knowledge or explicit acceptance. These communications could contain private or sensitive information and the sender will have a reasonable expectation that the recipient will keep the contents private.

190. Finally, given the ubiquitous nature of data storage systems, the apps on the device and the credentials stored on them may facilitate access to personal data stored in the cloud. This means the device is not just a repository of evidence in its own right, but it is also a key to wider personal information about the individual[227].

191. Using an extractive device, the police can obtain an extract of raw data which can be saved and analysed. Depending on the hardware and software used, an extraction report will be generated, allowing investigators to see at a glance a persons' location, who they speak to and when, and potentially vast amounts of other revealing information.[228]

192. There are different types of extraction: logical, file system and physical, which provide a framework to consider extraction technologies. While extraction technology has advanced rapidly in the past decade, no one technology can access and extract all data from all phones, and no one type of extraction is guaranteed to be successful.[229] Physical extraction is a bit-by-bit copy of the physical storage and entire filesystem of a device. Due to increasing sophistication of hardware encryption of mobile devices, especially iOS devices, physical extractions are complicated and take a long time. Logical extraction involves connecting the mobile device to forensic hardware or to a forensic workstation via a USB cable, a RJ-45 cable, infrared or Bluetooth. Forensic software can then extract raw data from the device.




227 Information Commissioner's Office Mobile phone data Extraction by police forces in England and Wales (2020) https://ico.org.uk/media/about-the-ico/documents/2617838/ico-report-on-mpe-in-england-and-wales-v1_1.pdf p. 13

228 https://privacyinternational.org/sites/default/files/201803/Digital%20Stop%20and%20Search%20Report.pdf

229 https://privacyinternational.org/sites/default/files/2019-10/A%20technical%20look%20at%20Phone%20Extraction%20FINAL.pdf

## PSNI PRACTICE OF MOBILE PHONE EXTRACTIONS

193. The PSNI has a Cyber Support Unit (CSU) that provides forensic MPE capability. The CSU has up to 60 full-time trained operators across four sites in Northern Ireland. These operators perform Mobile Phone Extractions, review the results and generate reports for the officer in charge (OIC) of the investigation, producing the digital evidential product. The operators also perform CCTV analysis. The PSNI Cyber Crime Centre in South Belfast is home to Digital Forensics and a Cyber Support Unit.[230] In the last quarter of 2022, 772 devices were examined.

194. In response to the ICO report in 2021, PSNI published a Mobile Phone Extraction Guidance in September 2022[231] and updated their application processes regarding MPE across the organisation. The guidance highlights the relevant legislation and explains how officers need to be clear whether it is referring to a consensual approach to engagement with a person to seek their agreement to examine their device or, alternatively, to the use of consent as a lawful basis for processing.[232] In most cases a suspect's device will have been acquired using a lawful power of seizure such as those conferred under PACE, but it is also possible that their device could be acquired by asking for their informed agreement.

195. The guidance also explains PSNI's MPE capabilities:

a. **Logical Extraction** – undertaken by a PSNI Cyber Support Unit (CSU) or Digital Forensics. The extraction software tool, CELLEBRITE, is deployed.
b. **File System Extraction** – undertaken by a PSNI CSU or Digital Forensics. The extraction software tool, CELLEBRITE, is deployed using a deeper analysis feature of the software.
c. **Physical Extraction** – undertaken by a PSNI CSU or Digital Forensics. The extraction software tool, CELLEBRITE, is deployed. This enables making a bit-for-bit copy of the contents of the device.
d. **Full File System** – Undertaken by CSU and Digital Forensics. There are 2 extraction tools available to recover data using this method. Usually deployed to service a more immediate need or to recover specific data types.

230 https://www.bbc.co.uk/news/uk-northern-ireland-48703072
231 PSNI Guidance relating to the lawful basis for conducting MPE within the PSNI (2022) https://www.psni.police.uk/sites/default/files/2022-09/Mobile%20Phone%20Extraction%20Guidance.pdf
232 ibid. p.11

196. **Taking a device from a suspect**

If needed for an investigation, officers will take possession of a digital device, such as a mobile phone or laptop. Investigating Officers won't extract information from the devices themselves but will send the device off to the examiners in the Cyber Support Unit. To this end, officers must fill out a 'Digital Processing Notice' (DPN) [233]. The DPN for a suspect's device contains information about the device and whether the suspect provided the device willingly or not. Furthermore, officers must provide reasonable grounds to believe that an examination of the device may find material relevant to the investigation and provide consideration whether it is strictly necessary to extract material from the device. Additionally, officers have to consider whether there is a risk of collateral intrusion (disclosing personal data of third parties).

197. The suspect will be furnished with a copy of the DPN, alongside a FAQ that answers the following questions:

- Why do the police need my device?
- Do I have to give my device to the police?
- How long will you keep my device for?
- Will the police look at everything on my device?
- What will the police do with the material they take from my device? Who will they give it to?
- How will my data be kept secure?
- Data Protection – what are my rights?

198. Taking a device from a witness or victim

Similarly, once a device has been supplied to PSNI by the victim or a witness, the investigating officer will fill out a DPN so that the phone can be examined by the Cyber Support Unit or Digital Forensics. Similarly, officers have to provide reasonable grounds to believe that an examination of the device may find material relevant to the investigation and provide consideration whether it is strictly necessary to extract material from the device. Officers also have to consider whether there is a risk of collateral intrusion (disclosing personal data of third parties). And in addition, officers must clarify whether any alternatives to extraction have been considered and to give an indication where the relevant material is likely to be stored on the device.

233 See Annex H and I for a sample digital processing notice and FAQ sheet.

199. The victim/witness is then also furnished with a copy of the DPN and a FAQ information sheet providing information on the following:

- The legal basis upon which the device is taken
- When PSNI will ask to look at the witness'/victim's device
- How PSNI will look at it
- What happens to the data PSNI copy, retain and review
- What might happen if the victim/witness does not agree
- Information and privacy rights

200. Several checks and balances are built in when officers make an application for a digital device examination: the supervising officer has to sign off, and if the examiner at the Cyber Support Unit or Digital Forensics feels the extraction is unnecessary or not proportionate, they discuss this with their supervisor in turn. Furthermore, the parameters for the search must be clearly defined and as narrow as possible. For example, a search for messages between the suspect and the victim for a particular period of time – officers will not be able to search a suspect's or witness's entire phone and message history.

201. The Cyber Crime location then owns the data. The phone data is subject to the usual data and retention schedule just as other evidence. After the investigation is closed, the data is retained per the schedule but not accessible, an officer would have to apply again to view the data.

202. As mentioned above, if there is another way of obtaining the data instead of extracting it from the device, officers will use that way. The PSNI thereby adhere to the judgement given in Bater-James.[234] If it is possible to be scheduled in that way, victim/witnesses can hand over their phone and the extraction will be done within a day so that they don't have to leave their phones. If there is a delay regarding persons getting their phone back, it is usually down to delays in the investigations or investigations being re-prioritized.

203. **Concerns**

The ICO states in their report that individuals may be worried that a decision not to consent will impact on the progress of their case, especially when the electronic devices are taken from victims of rape and sexual assault. Another concern is that a victim of sexual assault may also have their texts etc scrutinised for a period long before the assault in question to ascertain past sexual history.[235]

234 See Annex G for further analysis.

235 The Guardian, People who report rape face 'routine' demands for their mobile data, September 2019, https://www.theguardian.com/society/2019/sep/21/people-report-rape-routine-demands-mobile-data

In 2020, the National Police Chiefs' Council issued new forms and guidance, which set out the circumstances in which the police may lawfully ask a victim or witness to provide material from their digital devices in the course of a criminal investigation. However, this only came about after a legal challenge commenced by the Centre for Women's Justice in 2019. The legal challenge brought on behalf of two victims of serious sexual offences, set out how consent forms routinely issued to victims were unlawful, in policy and practice, and discriminated against women. Both claimants had been told that no criminal action could be taken against their attackers unless they agreed to full downloads of data from their mobile phones spanning several years.[236]

204. The Independent Reviewer of the Justice and Security Act has mentioned in her latest report that individuals and families who have been stopped and searched have had their devices taken and the property has never been returned, some individuals have experienced repeated seizures of equipment within a space of several months and, in some instances, receipts for the seizures have not been issued by police officers conducting the seizures.[237]

236 https://www.centreforwomensjustice.org.uk/news/2020/9/10/victory-for-victims-as-police-issue-new-digital-data-consent-forms

237 Report of the Independent Reviewer Justice and Security Act, Fourteenth Report, para 6.51, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1102689/E02756398_IRJSA_Report_Web_Accessible.pdf

# CHAPTER 8:
# DATA PROTECTION AT PSNI

205. This chapter lays out how PSNI manage data protection and privacy in their organisation. While data protection might be considered a dry subject, clear data protection principles and well-functioning data governance in an organisation are key to making sure that Article 8 rights are protected – in any organisation that holds personal/special category data about people's lives, but especially police services. As has been shown in the previous chapters, only someone that needs to access certain data to discharge their duties should be allowed to access certain data, about witnesses or suspects for example. For an overview of the principles laid out in the Data Protection Act, see Annex A, Data Protection Act.

## PSNI DATA PROTECTION PRINCIPLES

206. The Code of Ethics 3.1 on Privacy and confidentiality states that

> 'Police officers shall gather, retain, use and disclose information or data in accordance with the right to respect for private and family life contained in Article 8 of the European Convention on Human Rights and shall comply with all relevant legislation and Police Service policy and procedure governing the gathering, retention, use and disclosure of information or data'.[238]

Data Protection at the PSNI is applied via an extensive compliance framework including application of policy, guidance, mandatory training, monitoring, risk, incident and complaint management and reporting. PSNI furthermore adhere to the Home Office Code of Practice on the Management of Police Information[239], which sets out the principles for obtaining, recording, ownership, retention and deletion, sharing and protection of police information.

For the purposes of this report, we will focus mainly on compliance with Data Protection principles in this chapter.

207. One element of legislative compliance are Data Protection Impact Assessments (DPIAs). The PSNI Data Protection Service Instruction (SI) lays out how the Data Protection Act applies to the PSNI:

238 https://www.nipolicingboard.org.uk/files/nipolicingboard/publications/code-of-ethics.pdf
239 Code of Practice on the Management of Police Information, Home Office, 2005 https://library.college.police.uk/docs/APPref/Management-of-Police-Information.pdf

'One of the main ways in which this can be achieved is through the completion of Data Protection Impact Assessments (DPIAs). DPIAs are mandatory for certain types of projects or initiatives going forward that result in a high degree of risk to the rights and freedoms of individuals. This includes projects which intend to use large scale processing of special categories of data. This approach promotes data protection compliance from the start (i.e. by design). DPIA's ensure that technical measures are adopted as far as is practical/proportionate during the development of major IT systems to reduce the instances of poor quality data. Such measures may be informed by identification/reporting and rectification activities resulting from individuals exercising their right.' [240]

The SI also informs individuals how they can enact their individual rights, such as the right to access, erasure or rectification. These requests can be directed to the Corporate Information Branch of PSNI via Form DAT 3.[241]

The purpose of the SI is to:

- Provide protection to persons whose personal data is being processed by PSNI
- Set out PSNI procedures which are in place to secure compliance with the data protection obligations set out in Parts 2 and 3 of the DPA 2018; and
- Set out PSNI procedures which are in place to secure compliance with the data protection principles set out in Parts 2 and 3 of the DPA 2018; and
- Set out PSNI procedures which are in place to secure compliance with the data subjects rights set out in Parts 2 and 3 of the DPA 2018.

208. The PSNI Privacy Notice further clarifies which types of information the service may hold on individuals:[242]

- Personal details such as name, date of birth, address and biographical details
- Physical identifiers including DNA, fingerprints and other genetic samples
- Family, lifestyle and social circumstances
- Criminal proceedings, outcomes and sentences
- Religious or other beliefs of a similar nature
- Physical or mental health or condition
- Education and training details

240 https://www.psni.police.uk/sites/default/files/2022-09/Data%20Protection%2024%20May%202018.pdf
241 The Form can be accessed here: https://www.psni.police.uk/enacting-other-rights-under-data-protection-legislation
242 https://www.psni.police.uk/sites/default/files/2022-07/Adult%20Privacy%20Notices.pdf (note that this list is not exhaustive)

- Employment details
- Financial details
- Goods or services provided
- Racial or ethnic origin
- Political opinions
- Trade union membership
- Offences (including alleged offences)
- Sound and visual images
- Licenses or permits held
- Criminal Intelligence
- Sexual life/Sexual orientation
- References to manual records or files
- Complaint, incident and accident details

Data Subjects may be:

- Witnesses and victims
- Correspondents, enquirers and complainants
- Offenders and suspected offenders
- Personnel including permanent police officers and
- police staff, volunteers, agents, temporary and casual workers
- Relatives, guardians and associates of the individual concerned
- Other individuals necessarily identified in the course of police enquiries and activity
- Former and potential members of staff, pensioners and beneficiaries
- Advisers, consultants and other professional experts
- Suppliers

209. The PSNI retains information, including personal information, as long as the Service considers necessary for the purpose or purposes for which it was collected. The time periods are as detailed in the Service Review, Retention and Disposal Schedule, available online.[243]

210. Under Data Protection legislation, everyone has a right to know what kind of personal data is being processed by organisations, including police services. Everyone can make a Subject Access Request to PSNI by completing a Subject Access Request form (DAT1)[244] and emailing it to DataProtection@psni.police.uk.

243 https://www.psni.police.uk/sites/default/files/2022-07/Police%20Service%20of%20Northern%20Ireland%20-%20Review%2C%20Retention%20and%20Disposal%20Schedule%20V0.3.pdf
244 https://www.psni.police.uk/request/information-about-yourself

## DATA PROTECTION OFFICER (DPO)

211. The GDPR and Data Protection Act introduced a duty for data controllers such as the PSNI to appoint a data protection officer (DPO). Police forces such as PSNI are required to designate a DPO for general processing as police forces are 'Public Authorities' and for law Enforcement Processing as they are 'Competent Authorities'. The DPO must be independent, an expert in data protection, adequately resourced, and report to the highest management level. The Human Right's Advisor met with the PSNI's DPO in February 2023 where he was briefed on PSNI's data protection governance and how the DPO carries out their role.

212. Given that police services such as PSNI hold a lot of personal/special category data about many people, it is important that this data is adequately protected. Data protection governance ensures that data is shared lawfully and fairly in compliance with the DPA and personal/special category data is also only accessible to officers or other staff at PSNI who have a reason to see this data.

213. The overall task for any DPO is to achieve an understanding of the processing of personal data which occurs across an organisation and to consider if this processing is wholly compliant with legislation, identify where compliance can be strengthened, and risk further mitigated.[245] The DPO advises the PSNI Data Controller (Chief Constable) and the Senior Information Risk Owner (SIRO). The DPO is also the main point of contact with the Information Commissioner's Office. The ICO is the UK's independent body set up to uphold information rights and reports directly to Parliament. It is the national data protection authority dealing with the Data Protection Act 2018 and the General Data Protection Regulation, the Privacy and Electronic Communications (EC Directive) Regulations 2003 across the UK; and the Freedom of Information Act 2000 and the Environmental Information Regulations 2004 in England, Wales and Northern Ireland and, to a limited extent, in Scotland[246].

214. The ICO undertake audits of law enforcement agencies (LEAs), such as the PSNI, to investigate how well LEAs comply with data protection legislation. The ICO is doing a consensual audit in April and May 2023. The scope of the consensual audit is to assess PSNI's compliance in a number of areas agreed with ICO including data protection governance arrangements, business as usual DP processes, Mobile Phone Extraction and Rape and Serious Sexual Offenses.

245 https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-officers/#ib6
246 https://ico.org.uk/about-the-ico/what-we-do/

215. As part of the ongoing assessment of Data Protection related risks, the DPO monitors incidents and trends, for example system misuse. Incidents such as inappropriate access to information on the system will automatically inform the information security team and also triggers a Professional Standards process. The following table illustrates the percentage of officers who completed Data Protection training, how many data protection incidents occurred in the given month and whether these were incidents notifiable to ICO.

| DPO Functions | 01.09.22 – 30.09.22 | 01.10.22 – 31.10.22 | 01.11.22 – 30.11.22 | 01.12.22 – 31.12.22 | 01.01.23 – 31.01.23 | 01.02.23 – 28.02.23 |
|---|---|---|---|---|---|---|
| DP Training Completion | 91.9% | 95% | 95.9% | 95.9% | 97.5% | 97.5% |
| Incidents 'not notified to ICO' | 9 | 14 | 18 | 10 | 11 | 7 |
| Incidents 'notified to ICO' | 1 | 2 | 2 | 1 | 0 | 2 |
| Complaints 'Received' | 2 | 1 | 1 | 3 | 5 | 1 |
| DPIAs 'Responded to' | 4 | 4 | 4 | 5 | 7 | 1 |

Every 2 years a full online Data Protection Compliance survey is carried out with PSNI officers and staff. Each survey results in an Action Plan to improve compliance and reduce risk. The DPO also provides advice regarding Data Protection Impact Assessments (DPIAs). DPIAs are mandatory for certain types of projects or initiatives going forward that result in a high degree of risk to the rights and freedoms of individuals. This includes projects which intend to use large scale processing of special categories of data[247]. The DPO and operational leads sign off on these DPIAs.[248]

PSNI also produces Privacy Impact Assessment for major projects, such as Body Worn Video (BWV) and ANPR.

247 More information can be found in the Data Protection Service Instruction.
248 See Annex J for a list of DPIAs.

# ANNEX A

# OVERVIEW OF THE CASE LAW ON HUMAN RIGHTS AND DATA PROTECTION LEGISLATION

This Annex provides an overview of the case law regarding Article 8 ECHR, the right to privacy and an overview of the Data Protection Act 2018.[249]

However, as noted in the introduction PSNI also have positive duties to protect lives and prevent ill-treatment:

'a positive obligation on the authorities to take preventive operational measures to protect an individual whose life is at risk from the criminal acts of another individual…

such an obligation must be interpreted in a way that does not impose an impossible or disproportionate burden…

to ensure that the police exercise their powers to control and prevent crime in a manner which fully respects the due process and other guarantees which legitimately place restraints on the scope of their action to investigate crime and bring offenders to justice, including the guarantees contained in Articles 5 and 8 of the Convention…

For a positive obligation to arise it must be established that the authorities knew or ought to have known at the time of the existence of a real and immediate risk to life of an identified individual or individuals…'[250]

These duties may apply, for instance, in using CCTV systems to find vulnerable people who are at 'immediate risk'.

### Article 8 of the Convention– Right to respect for private and family life

"1. Everyone has the right to respect for his private and family life, his home and his correspondence. 2. There shall be no interference by a public 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

249 Note that virtually every substantial international human rights treaty includes a right to privacy and that all these treaties have been ratified by the UK and, as a result, they are binding on law enforcement agencies in Northern Ireland as a matter of international law.

250 ECtHR Guide to Article 2, paras 16, 17, 18 and 19. See also the Guide to Article 3, para 106 onwards which sets out the same principles.

wellbeing 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."

The following overview is mainly adapted from the ECtHR guidance on Article 8[251] and the case law guidance regarding data protection.[252]

Article 8 covers four areas, namely: private life, family life, home and correspondence. Some matters, of course, span more than one interest. The primary purpose of Article 8 is to protect against arbitrary interferences with private and family life, home, and correspondence by a public authority.[253]

Conditions upon which a State may interfere with the enjoyment of a protected right are set out in paragraph 2 of Article 8, namely in the interests of national security, public safety, or the economic wellbeing 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. Limitations are allowed if they are "in accordance with the law" or "prescribed by law" and are "necessary in a democratic society" for the protection of one of the objectives set out above. In the assessment of the test of necessity in a democratic society, the Court often needs to balance the applicant's interests protected by Article 8 and a third party's interests protected by other provisions of the Convention and its Protocols.

The ECtHR has developed a threefold test to assess whether an interference is in accordance with the law. First, the interference must have a basis in national law, second, the law must be accessible, and third, the law must be sufficiently foreseeable to enable individuals to act in accordance with the law.[254] This does not mean that one has to be advised in advance whether one's data is about to be accessed, as this could defeat the purpose, rather, it means that the rules of the system are clear to all.

### Is the interference in accordance with the law?

Any interference by a public authority with an individual's right to respect for private life, family life, home and correspondence must be with in accordance with the law.[255] This expression does not only necessitate compliance with domestic law but also relates to the quality of that law, requiring it to be compatible with the rule of law.[256]

251 https://www.echr.coe.int/documents/guide_art_8_eng.pdf
252 https://www.echr.coe.int/Documents/Guide_Data_protection_ENG.pdf
253 *Libert v. France*, paras 40-42
254 Silver and Others v United Kingdom 1983, para 87
255 see notably Vavřička and Others v. the Czech Republic [GC], paras 266-269 and the notion of "law" under the Convention; Klaus Müller v. Germany, paras 48-51
256 Big Brother Watch and Others v. the United Kingdom [GC] para 332.

The Court has repeatedly set out that the national law must be clear, foreseeable, and adequately accessible[257]. It must be sufficiently foreseeable to enable individuals to act in accordance with the law and it must clearly demarcate the scope of discretion for public authorities. For example, as the Court formulated in the surveillance context, the law must be sufficiently clear in its terms to give citizens an adequate indication of the conditions and circumstances in which the authorities are empowered to resort to any measures of secret surveillance and collection of data[258].

### Is the interference "necessary in a democratic society"?

To determine whether a particular infringement upon Article 8 is "necessary in a democratic society" the Court balances the interests of the Member State against the right of the applicant. "Necessary" in this context implies the existence of a "pressing social need" for the interference in question. It is for national authorities to make the initial assessment of the pressing social need in each case; accordingly, a margin of appreciation is left to them. However, their decision remains subject to review by the Court. A restriction on a Convention right cannot be regarded as "necessary in a democratic society" unless, amongst other things, it is proportionate to the legitimate aim pursued[259].

The Council of Europe Policing Handbook explains this further:

'From a policing perspective, it is important to ensure that adequate measures are in place to ensure compliance both with national law and with the European Convention on Human Rights. For example, if national law allows for the exercise of police powers in a very broad range of scenarios, police officers responsible for their exercise should ensure that they only use the powers where there is a demonstrated need, and for their proper purpose. This will assist in reducing the likelihood of a successful legal challenge, either in the domestic courts or in Strasbourg.'[260]

The right to privacy is similarly qualified under Article 17 of the International Covenant on Civil and Political Rights ('ICCPR').

The United Nations Special Rapporteur on the right to privacy has set out a four-fold test that any legitimate infringement of privacy cannot be:

257 Silver and Others v. the United Kingdom, para 87; for an instruction issued by the Chief Prosecutor, see Vasil Vasilev v. Bulgaria, paras 92-94; for instructions issued by the Ministry of Justice, see Nuh Uzun and Others v. Turkey, para 83-99

258 See for example S. and Marper v. the United Kingdom [GCpara 95, ECHR 2008 and Kennedy v United Kingdom 2010, para 151

259 *Dudgeon v. the United Kingdom*, paras 51-53

260 https://www.echr.coe.int/documents/handbook_european_convention_police_eng.pdf

"(a) arbitrary and must be provided for by law;
(b) for any purpose but for one which is necessary in a democratic society;
(c) for any purpose except for those of "national security or public safety, public order, the protection of public health or morals or the protection of the rights and freedoms of others"; and,
(d) the measure must be proportionate to the threat or risk being managed."[261]

### Definition of private life

Private life is a broad concept incapable of exhaustive definition[262]. It covers the physical and psychological integrity of a person and may "embrace multiple aspects of the person's physical and social identity"[263].

The notion of private life is not limited to an "inner circle" in which the individual may live his own personal life as he chooses and exclude the outside world.[264] Article 8 protects the right to personal development, whether in terms of personality or of personal autonomy, which is an important principle underlying the interpretation of the Article 8 guarantees. It encompasses the right for each individual to approach others in order to establish and develop relationships with them and with the outside world, that is, the right to a "private social life"[265].

The Court has also held that the concept of "private life" extends to aspects relating to personal identity, such as a person's name, photo, or physical and moral integrity[266]; the guarantee afforded by Article 8 is primarily intended to ensure the development, without outside interference, of the personality of each individual in his relations with other human beings.

Since Article 8 guarantees the right to a "private social life", it may, under certain circumstances, include professional activities[267], and commercial activities[268]. Private life encompasses the right for an individual to form and develop relationships with other human beings, including relationships of a professional or business nature[269].

261 United Nations Human Rights Council, Report of the Special Rapporteur on the right to privacy
262 *Niemietz v. Germany*, para 29; *Pretty v. the United Kingdom*, para 61; *Peck v. the United Kingdom*, para 57
263 *Denisov v. Ukraine* [GC], para 95; *S. and Marper v. the United Kingdom* [GC], para 66
264 *Denisov v. Ukraine* [GC], para 96
265 *Bărbulescu v. Romania* [GC], para 71; *Botta v. Italy*, para 32
266 *Vavřička and Others v. the Czech Republic* [GC], para 261
267 *Fernández Martínez v. Spain* [GC], para 110; *Bărbulescu v. Romania* [GC], para 71; *Antović and Mirković v. Montenegro*, para 42; *Denisov v. Ukraine* [GC], paras 100 with further references therein and *López Ribalda and Others v. Spain* [GC], paras 92-95
268 *Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland* [GC], para 130
269 *C. v. Belgium*, para 25; *Oleksandr Volkov v. Ukraine*, para 165

### Online activities

Regarding online activities, information associated with specific dynamic IP addresses facilitating the identification of the author of such activities, constitutes, in principle, personal data which are not accessible to the public. The use of such data may therefore fall within the scope of Article 8[270]. In that regard, the fact that the applicant had not concealed his dynamic IP address had not been a decisive factor for assessing whether his expectation of privacy had been reasonable (para 116). Conversely, the anonymity linked to online activities is an important factor which must be taken into account (para 117).

### Data collection by public authorities

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.[271]

The Court has found breaches of Article 8 in the following cases: recording of the applicants' voices when they were being charged and while they were being held in their cells at the police station[272]; the filming, for identification purposes, of a suspect in a police station using a covert closed-circuit camera[273]; the recording by the police, by means of a listening device installed in the home of a third person whom the applicant had visited, of an unprompted, spontaneous conversation during which the applicant had admitted that he had been a party to the importation of drugs[274]; police bugging of private premises in the framework of a judicial investigation[275]; recording of a conversation by means of a listening device planted on the person by the police authorities, and the subsequent use of that recording at the trial, albeit not as the only item of incriminating evidence[276]; and the recording of communications by an individual in the context and for the benefit of an official investigation, whether criminal or of another nature, with the co-operation and technical assistance of the State investigative authorities[277].

270 *Benedik v. Slovenia*, paras 107-108
271 *Peck v. the United Kingdom*, 2003, paras 59-62; *Perry v. the United Kingdom*, 2003, paras 41-42
272 *P.G. and J.H. v. the United Kingdom*, 2001, paras 56-63
273 *Perry v. the United Kingdom*, 2003, paras 36-49
274 *Khan v. the United Kingdom*, 2000, paras 25-28
275 *Vetter v. France*, 2005, paras 20-27
276 *Heglas v. Czech Republic*, 2007, paras 71-76
277 *Van Vondel v. the Netherlands*, 2007, paras 47-55

### Public surveillance

With respect to surveillance and the collection of private data by agents of the State, such information, when systematically collected and stored in a file held by agents of the State, falls within the scope of "private life" for the purposes of Article 8 para 1 of the Convention.

Since there are occasions when people knowingly or intentionally involve themselves in activities which are or may be recorded or reported in a public manner, a person's reasonable expectations as to privacy may be a significant, although not necessarily conclusive, factor[278]. A person who walks down the street will, inevitably, be visible to any member of the public who is also present. Monitoring by technological means of the same public scene (for example, a security guard viewing through closed-circuit television) is of a similar character. Private life considerations may arise, however, once any systematic or permanent record comes into existence of such material from the public domain. It is for this reason that files gathered by security services on a particular individual fall within the scope of Article 8, even where the information has not been gathered by any intrusive or covert method[279].

For example, in Peck v the United Kingdom, the applicant had been unaware that he was being filmed by a closed-circuit television at the point where he attempted to commit suicide in a deserted public street, but the filming had allowed the police to render medical assistance. Subsequently, the local administration after obtaining copies of the tapes had released still photographs and video footage of the immediate aftermath of the incident to portray the advantages of CCTV. This material had appeared in newspapers and on television and had allowed the applicant to be identified. For the Strasbourg Court, while the monitoring by means of photographic equipment of the actions of an individual in a public place would not in itself amount to an interference with private life, the recording of data in a systematic or permanent manner could well do so. Here, the incident had been seen to an extent which far exceeded any exposure to a passer-by or to security observation, and had been to a degree surpassing what the applicant could reasonably have foreseen. The disclosure thus involved a serious interference with the right to respect for his private life, and in the circumstances had also constituted a violation of Article 8 as there had not been relevant and sufficient reasons to justify the direct disclosure of material without obtaining the applicant's consent or masking his identity.

278 *Benedik v. Slovenia*, para 101
279 *P.G. and J.H. v. the United Kingdom*, para 57

## Covert surveillance

In its first judgment concerning secret surveillance, *Klass and Others v. Germany*, para 48, the Court stated, in particular: "Democratic societies nowadays find themselves threatened by highly sophisticated forms of espionage and by terrorism, with the result that the State must be able, in order effectively to counter such threats, to undertake the secret surveillance of subversive elements operating within its jurisdiction. The Court has therefore to accept that the existence of some legislation granting powers of secret surveillance over the mail, post and telecommunications is, under exceptional conditions, necessary in a democratic society in the interests of national security and/or for the prevention of disorder or crime." However, powers of secret surveillance of citizens, characterising as they do the police state, are tolerable under the Convention only in so far as *strictly necessary* for safeguarding the democratic institutions[280]. In the latter case, the Court clarified the concept of "strict necessity". Thus, a measure of secret surveillance must, in general, be strictly necessary for the safeguarding of democratic institutions and, in particular, for the obtaining of vital intelligence in an individual operation.

The Court has held that where a State institutes secret surveillance, the existence of which remains unknown to the persons being controlled with the effect that the surveillance remains unchallengeable, individuals could be deprived of their Article 8 rights without being aware and without being able to obtain a remedy either at the national level or before the Convention institutions[281]. This is especially so in a climate where technological developments have advanced the means of espionage and surveillance, and where the State may have legitimate interests in preventing disorder, crime, or terrorism[282].

The mere existence of legislation which allows a system for the secret monitoring of communications entails a threat of surveillance for all those to whom the legislation may be applied[283]. While domestic legislatures and national authorities enjoy a certain margin of appreciation in which to assess what system of surveillance is required, States do not enjoy unlimited discretion to subject persons within their jurisdiction to secret surveillance[284]. The Court has affirmed that States may not, in the name of the struggle against espionage and terrorism, adopt whatever measures they deem appropriate; rather, whatever system of surveillance is adopted, there must be adequate and effective guarantees against abuse[285].

280 ibid., para 42; *Szabó and Vissy v. Hungary*, paras 72-73
281 *Klass and Others v. Germany*, para 36
282 ibid., para 48
283 *Weber and Saravia v. Germany* (dec.), para 78
284 *Zoltán Varga v. Slovakia*, 2021, para 151
285 *Weber and Saravia v. Germany* (dec.), para 106, *Khan v. the United Kingdom*, paras 26-28

Powers of secret surveillance of citizens are tolerable only in so far as strictly necessary for safeguarding the democratic institutions[286]. Such interference must be supported by relevant and sufficient reasons and must be proportionate to the legitimate aim or aims pursued[287].

This means that the surveillance measure must have some basis in domestic law and be compatible with the rule of law. The law must therefore meet quality requirements: it must be accessible to the person concerned and foreseeable as to its effects[288]. In the context of the interception of communications, "foreseeability" cannot be understood in the same way as in many other fields. Foreseeability in the special context of secret measures of surveillance cannot mean that individuals should be able to foresee when the authorities are likely to intercept their communications so that they can adapt their conduct accordingly[289]. However, to avoid arbitrary interference, it is essential to have clear, detailed rules on the interception of telephone conversations. The law must be sufficiently clear to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to any such secret measures[290]. In addition, the law must indicate the scope of the discretion granted to the executive or to a judge and the manner of its exercise with sufficient clarity to give the individual adequate protection against arbitrary interference[291].

The Council of Europe Policing Handbook states: 'A general power to take steps necessary for the investigation of crime is not a sufficient basis for specific measures, such as the interception of telecommunications. It is necessary that the law contain provisions concerning the precise circumstances under which telecommunications can be intercepted, for what purpose any conversations recorded may be used and for how long they may be retained. In addition, it serves to ensure that persons are able to foresee, with a degree of accuracy, the circumstances in which they may be subjected to the exercise of such powers.'[292]

A law on measures of secret surveillance must provide the following minimum safeguards against abuses of power: a definition of the nature of offences which may give rise to an interception order and the categories of people liable to have their telephones tapped; a limit on the duration of the measure; the procedure to be followed

286 *Klass and Others v. Germany*, para 42; *Szabó and Vissy v Hungary*, paras 72-73
287 *Segerstedt-Wiberg and Others v. Sweden*, para 88
288 *Kennedy v. the United Kingdom*, para 151; *Roman Zakharov v. Russia* [GC], para 229
289 *Weber and Saravia v. Germany*, para 93
290 *Roman Zakharov v. Russia* [GC], para 229; *Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria*, para 75
291 *Roman Zakharov v. Russia*, para 230; *Malone v. the United Kingdom*, para 68; *Huvig v. France*, para 29; *Weber and Saravia v. Germany* (dec.), para 94
292 https://www.echr.coe.int/documents/handbook_european_convention_police_eng.pdf

for examining, using and storing the data obtained; the precautions to be taken when communicating the data to other parties; and the circumstances in which recordings may or must be erased or destroyed[293].

When balancing the respondent State's interest in protecting its national security through secret surveillance measures against the seriousness of the interference with an applicant's right to respect for his or her private life, the national authorities enjoy a certain margin of appreciation in choosing the means for achieving the legitimate aim of protecting national security. However, there must be adequate and effective safeguards against abuse. The Court thus considers the circumstances of the case, such as the nature, scope and duration of the possible measures, the grounds required for ordering them, the authorities competent to authorise, carry out and supervise them, and the kind of remedy provided by the national law[294].

### Data transfer

The case of *Big Brother Watch and Others v. the United Kingdom* [GC], 2021 raised, *inter alia*, the question of the compatibility with Article 8 of the Convention of the sharing of data intercepted by foreign intelligence services, in this case the US National Security Agency ("NSA"). The Court stated that the exchange of data had to be framed by clear detailed rules which gave citizens an adequate indication of the circumstances in which and the conditions on which the authorities were empowered to make such requests and which provided effective guarantees against the use of this power to circumvent domestic law and/or the States' obligations under the Convention. Upon receipt of the intercept material, the receiving State must have in place adequate safeguards for its examination, use and storage; for its onward transmission; and for its erasure and destruction. These safeguards were equally applicable to the receipt, by a Contracting State, of solicited intercept material from a foreign intelligence service. If States did not always know whether material received from foreign intelligence services was the product of interception, then the Court considered that the same standards should apply to all material received from foreign intelligence services that could be the product of intercept. Finally, any regime permitting intelligence services to request either interception or intercept material from non-Contracting States should be subject to independent supervision, and there should also be the possibility for independent *ex post facto* review[295].

293 *Roman Zakharov v. Russia* [GC], paras 231 and 238-301; *Amann v. Switzerland* [GC], paras 56-58
294 *Roman Zakharov v. Russia* [GC], para 232; *İrfan Güzel v. Turkey*, para 85, *Ekimdzhiev and Others v. Bulgaria,* paras 418 and 419[f]; see also *Big Brother Watch and Others v. the United Kingdom* [GC]; *Centrum för rättvisa v. Sweden* [GC])
295 ibid. paras 498-499

There is a tension between meaningfully vindicating individual rights and permitting law enforcement authorities to use and access technology to address the commission of serious crime, however, the state must endeavour to balance the different rights at play.[296]

### Data Protection Act

The DPA 2018 sets out the data protection framework in the UK, alongside the UK GDPR. It contains three separate data protection regimes:

Part 2: sets out a general processing regime (the UK GDPR);
Part 3: sets out a separate regime for law enforcement authorities; and
Part 4: sets out a separate regime for the three intelligence services[297].

When undertaking law enforcement processing, the DPA 2018 makes data controllers responsible for, and requires that they be able to demonstrate compliance with, the following principles[298]:

- First principle: The processing must be lawful and fair.
  For the processing to be lawful, section 35(2) says that it must be "based on law". Law enforcement must identify a legal basis that provides a sufficiently clear, precise and foreseeable lawful justification to process personal data for the law enforcement purposes.
  The processing must also have a lawful basis under data protection legislation. Section 35(2) explains that the processing of personal data for any of the law enforcement purposes must be either necessary for the performance of a task carried out for law enforcement purposes by a competent authority, or based on consent.[299]
- Second principle: The processing must be limited to a specified, explicit and legitimate purpose, and it must not be processed in a manner that is incompatible with the purpose for which it was collected.
- Specific requirements about the purpose being specified, explicit and legitimate are introduced, meaning that any processing under Part 3 of the DPA 2018 must be for the defined law enforcement purposes. Data cannot be processed for a purpose that is incompatible with the original reason and justification for processing.

296 There is a positive obligation on authorities to investigate crimes, which constitutes an element of the right to an effective remedy under Article 13 ECHR and as a procedural element of the right to life, the right to freedom from torture and ill-treatment, and the right to respect for private life amongst other core civil rights. See Osman v UK 1998.
297 https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted
298 ss35-40 DPA 2018
299 https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-le-processing/principles/

- Third principle: The data must be adequate, relevant, and not excessive in relation to the purpose for which it is processed.
- Fourth principle: The data must be accurate and, where necessary, kept up to date, and every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the law enforcement purpose for which it is processed, is erased or rectified without delay. In addition, as far as possible, a clear distinction must be made between different categories of individuals – those suspected of an offence, those convicted, witnesses and complainants. Personal data based on fact must as far as possible be distinguished from personal data based on personal assessments.
- Fifth principle: Data should be stored for no longer than is necessary, and appropriate limits must be set for periodic review of the need for continued storage.
- Sixth principle: There must be adequate measures in place to ensure the appropriate security of data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage In the context of law enforcement processing, there are additional protections where the data is considered to be 'sensitive'.

'Sensitive processing' is defined as the processing of:

- 'personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership;
- genetic data, or of biometric data, for the purpose of uniquely identifying an individual;
- data concerning health; or
- data concerning an individual's sex life or sexual orientation.[300]' Sensitive processing requires law enforcement to have an 'appropriate policy document' in place.

The conditions for sensitive processing in Schedule 8 of the Act are:

- necessary for judicial and statutory purposes – for reasons of substantial public interest;
- necessary for the administration of justice;
- necessary to protect the vital interests of the data subject or another individual;
- necessary for the safeguarding of children and of individuals at risk;
- personal data already in the public domain (manifestly made public);
- necessary for legal claims;

300 s35(8) DPA 2018

- necessary for when a court acts in its judicial capacity;
- necessary for the purpose of preventing fraud; and
- necessary for archiving, research or statistical purposes.

S35 DPA 2018 mandates the requirement for an appropriate policy document to be in place before sensitive processing is undertaken and for this processing to be either:

- with the consent of the data subject (within the meaning of data processing law); or
- strictly necessary for the law enforcement purpose and meeting a condition in Schedule 8 DPA 2018.

The processing can be lawful only if and to the extent that it is based on law and either:

- the data subject has given consent (within the meaning of data processing law) to the processing for that purpose; or
- the processing is necessary for the performance of a task carried out for that purpose by a competent authority.

In all cases where sensitive data may be involved, an appropriate policy document, describing how sensitive data is handled and what safeguards are applied, must be in place.

If an interference with Article 8 rights (ie respect for private and family life, home and correspondence) is to be justified, it must meet a four-part test[301], namely whether:

1. the objective of the measure pursued is sufficiently important to justify the limitation of a fundamental right;
2. it is rationally connected to the objective;
3. a less intrusive measure could have been used without unacceptably compromising the objective; and
4. having regard to these matters and to the severity of the consequences, a fair balance has been struck between the rights of the individual and the interests of the community.

In all cases where sensitive data may be involved (regardless of the lawful basis relied upon), police forces must have in place an appropriate policy document, describing how sensitive data is handled and what safeguards are applied[302].

301 Bank Mellat v Her Majesty's Treasury (No 2) https://www.bailii.org/uk/cases/UKSC/2013/39.html
302 https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/special-category-data/

Furthermore, Part 3, Chapter 3 of the Act provides the following individual rights:

- the right to be informed;
- the right of access;
- the right to rectification;
- the right to erasure or restrict processing; and
- the right not to be subject to automated decision-making.

## ANNEX B

# EXTRACTS FROM THE HUMAN RIGHTS ANNUAL REPORTS 2020/21[303] AND 2021/22 REGARDING BIOMETRIC RETENTION[304]

### The current problems of biometric retention

The Grand Chamber of the European Court of Human Rights (ECtHR) decided, in the 2008, the case of S and Marper v UK, challenging the blanket policy of retaining indefinitely the DNA samples, profiles and fingerprints (referred to collectively as 'biometric material') of all people who have been arrested, but not convicted of an offence. The Court found that this policy did not comply with the right to respect for private and family life (Article 8). In response to the Marper judgment the Northern Ireland Assembly introduced a new legislative framework for the retention and destruction of biometric material - the Criminal Justice Act (Northern Ireland) 2013. There was, however, a delay in the new framework coming into operation, but as an interim measure PSNI established a Biometric Retention/Disposal Ratification Committee which met regularly to discuss applications for individuals requesting that their biometric materials be destroyed and relevant records and databases amended to reflect this.

In January 2019 the Northern Ireland Human Rights Commission reported that it had settled a case taken against PSNI on DNA retention.[305] As a result the PSNI agreed to produce a formal public policy on the retention of biometric data within 12 months. The policy was designed to take into account human rights and to provide guidance to the public on how they can find out if their DNA or fingerprints have been retained, why this is so, and how they can challenge the decision if necessary.

In the continued absence of legislation, the PSNI's proposal was that its new Service Instruction would come into force in April 2020 and would be modelled on the provisions of the Criminal Justice (Northern Ireland) Act 2013 (the CJA), although that

303 https://www.nipolicingboard.org.uk/files/nipolicingboard/publications/human-rights-annual-report-2020-2021.pdf
304 https://www.nipolicingboard.org.uk/files/nipolicingboard/2023-01/human-rights-annual-report-21-22_0.pdf
305 9th January 2019, https://nihrc.org/news/detail/human-rights-commission-secures-settlement-in-dna-fingerprint-retention-cas

Act had still not yet come into force. In accordance with proposals from the NIO, the PSNI intended to take a digital and hard copy "snapshot" of the undeleted fingerprints and DNA databases and pass this over to the proposed Historical Investigations Unit (HIU).[306] The plan being, that separate legislation would restrict access to this snapshot, making it only available to the proposed HIU's investigations.[307]

The draft Service Instruction and draft Guidance were driven by the positive desire to make the biometric retention regime more human rights compliant and, substantially, to reduce the numbers of people who have their data retained.

In February 2019 the ECtHR gave its judgment in a case challenging the retention policies of the PSNI (and of police services across the UK). The Court was particularly helpful in its judgment in giving guidance as to how a compliant system in the UK might be structured in the future.[308] The keys to lawful retention appear to be:

- To take account of the domestic rules on the threshold for convictions being "spent";
- To ensure that the new regime takes account of the seriousness of the offence and any continuing need to retain the biometric material for policing and criminal reasons;[309]
- A real process of review to allow individuals to seek deletion of their data, including taking into account possible changes in their personality (and presumably the likelihood of committing further offences);
- Taking into account the age of the person when he or she was convicted and the length of time between the offence and the end of retention period; and
- Noting that the new separate regime for the deletion of photographs in the UK allows deletion after six years for people convicted of less serious recordable offences.

A consultation was held by the Department of Justice between July and August 2020 on new proposals to amend the legislation governing the retention of DNA and fingerprints in Northern Ireland. The Department proposed policy changes in five key areas, each of these are summarised below and these were largely confirmed in its report in October 2020.[310]

306 This was intended to mitigate the risk posed to historical enquiries by the deletion of material as a result of CJA commencement.
307 The Northern Ireland (Stormont House Agreement) Bill.
308 *Gaughran v UK* paras 94 - 96
309 It might be argued that retaining biometric data is of no help in dealing with offenders who drink and drive.
310 A Consultation on Proposals to Amend the Legislation Governing the Retention of DNA and Fingerprints in Northern Ireland: Summary of Responses.

The Department proposed legislative amendments to replace the indefinite retention elements of the CJA with maximum periods of retention for convictions based on the seriousness of the offence and the age of the offender, as below:

- 75 years retention period for DNA and fingerprints for all convictions associated with serious violent, sexual and terrorism offences ("qualifying offences")
- 50 years retention period for adult convictions for recordable offences that do not fall within the serious category; and
- 25 years retention period for 2 or more juvenile non-serious convictions which do not involve a custodial sentence of more than 5 years (an under 18 conviction for a non-serious offence involving a custodial sentence of more than 5 years will attract a 50 years retention period).

The Department proposed to make provision within the Act for a regulation-making power that will enable the Department to set out clearly in secondary legislation a detailed review mechanism that will apply to all material failing within the 75/50/25 year's maximum retention periods.

They envisage that the Regulations will include:

- Detail on the review periods;
- The criteria to be applied;
- Who will conduct the review;
- How it will be conducted;
- How individuals can request a review of their retained data.

The Department proposed to amend the Act to enable DNA and fingerprints that are taken under PACE NI in connection with an offence in Northern Ireland to be retained on the basis of a conviction for a recordable offence committed in a country or territory outside the United Kingdom.

It was proposed that the relevant material would be retained under a simplified version of the retention model for convicted persons that is set out in the first policy proposal. This would involve a maximum retention period of 50 years for adult convictions and 25 years for under 18 convictions for offences committed outside the UK. The Department do not propose to use the concept of qualifying offences as they are unique to the UK biometrics legislation and it would be a complex exercise to attempt to map serious offences committed in other countries to the list set out in Northern Ireland legislation.

The Department proposed to amend CJA to enable the DNA and fingerprints taken in connection with an offence that has been 'left on books' by the court to be retained for a period of 12 months from the date in which the judge consents for the charge to be 'left on books' – this refers to the scenario where the PPS makes a case to the court to not proceed with a particular charge but for it to be 'left on books'. The judge may then decide at a later date, possibly as a result of a further criminal action, to resurrect the charge and continue with criminal proceedings in relation to this offence.

In effect, if DNA and fingerprints are taken in connection with an offence which is subject to an order by a judge to be 'left on books' and there is no other basis under the Criminal Justice Act for the material to be retained (for example, a previous conviction) then the biometric material must be destroyed. This proposal will ensure that material is not destroyed until a sufficient time period has lapsed to indicate that the charge is unlikely to be resurrected by the court.

The Department proposed to make provision within CJA to widen the scope of the Northern Ireland Commissioner for the Retention of Biometric Material (the Commissioner) to provide independent statutory oversight of the acquisition, retention, use and disposal of biometric material in accordance with Article 63B to 63R of PACE NI. The Department also wishes to broaden that scope to include keeping under review existing, emerging and future biometrics for use by the PSNI and other public bodies for law enforcement purposes.

Under the current provisions of Schedule 2 of CJA, the Commissioner's sole function was to consider applications from the PSNI for the retention of DNA and fingerprints from persons arrested, but not charged with a serious offence and where so called 'prescribed circumstances' apply. This was to be an exception to the overall retention architecture and was opposed by some MLA Members when the 2013 Act was considered by the Assembly. The retention of biometric material by the PSNI of a person not convicted of an offence is unlikely to comply with Article 8.

The Department proposed to amend CJA to require the NI Commissioner to report annually, and also as necessary to them and for the Department to publish and lay reports in the Assembly. This reflects the wider statutory role of the Commissioner for the retention and use of biometric material in England and Wales.

### Retention for Legacy Cases

In the Gaughran case, the UK Government made a particular submission to the ECtHR in relation to the need to keep biometric data to enable the authorities to use that data to investigate the significant numbers of deaths during the Troubles that have not yet

been properly investigated.[311] As set out above, the intention was to take a "snapshot" of the complete database before any deletions occur, (the deletions necessary as a result of S and Marper) but to restrict access to this snapshot to those investigating these deaths from the past. The UK has continuing investigatory obligations in these so-called McKerr group of cases.[312] In those cases the Court found violations of the investigatory duty under Article 2 and these cases are still subject to the supervision of the Committee of Ministers.[313] However, this particular plea to retain the "snapshot" was rejected in Gaughran v UK, albeit that the Court accepted that it was not for them to decide this point, but stating the principle that:

'… in the context of unlawful killings the Court has underlined that the police must discharge their duties in a manner which is compatible with the rights and freedoms of other individuals. Indeed, without respect for the requisite proportionality visàvis the legitimate aims assigned to such mechanisms, their advantages would be outweighed by the serious breaches which they would cause to the rights and freedoms which States must guarantee under the Convention to persons under their jurisdiction.'[314]

However, the Northern Ireland Troubles (Legacy and Reconciliation) Bill, published in May 2022, includes a provision that would give the Secretary of State the power to retain this snapshot for purposes of investigations by the Independent Commission for Reconciliation and Information Recovery (ICRIR) – which is to be established once the Bill is officially enacted - and argues:

'108. The Department considers that, notwithstanding the observations of the Court in *Gaughran*, the exercise of the power created by clause 30 to provide for the retention of legacy biometrics is compatible with Article 8. In *Gaughran* the Court was not directly concerned with the proposal contemplated in this Bill, but rather a legislative regime in which biometrics were retained for the general purpose of prevention and detection of all crime. Further, the Court seemed to assume that Troubles-related "cold cases" were like any other – a comparison which the Department does not consider to be apt, and, importantly, *Gaughran* is a single chamber judgment and does not represent a clear and consistent line of decisions.

109. The Department is satisfied there is a strong evidential basis for the proposed retention of legacy biometrics under clause 30, as an exception to the post *Marper/ Gaughran* general retention regime.

311 See Schedule 8 of the Draft Northern Ireland (Stormont House Agreement) Bill
312 McKerr v UK (2001).
313 See the Department for the Execution of Judgments of the European Court of Human Rights, UK Country report on these cases, https://hudoc.exec.coe.int/eng#{"EXECIdentifier":["004-2202"]}
314 Para. 93 and see Osman v UK (1998).

110. The historical nature of the deaths with which the ICRIR is concerned - deaths and serious injuries between 1968 and 1998 - create particular difficulties because the evidential trail has significantly narrowed. Advice received by the Northern Ireland Office from an experienced senior operational officer, charged with managing legacy investigations on behalf of the PSNI, is that forensic evidence is "the strongest single strand in legacy investigations". Having analysed the specific challenges in relying on other strands of evidence in historic murder investigations, he concluded that "unlike the other strands, [forensic evidence] is capable of providing corroborative evidence which is not impacted by fear, memory fade or organisational capacity. This creates the potential for offenders to be identified and prosecuted successfully." Even though investigations carried out by the ICRIR will not result in prosecutions in cases where immunity is granted, they are still the State's way of carrying out Article 2 compliant investigations into deaths, and this justification therefore applies equally to ICRIR investigations.

111. The kinds of incidents with which the ICRIR is concerned, many of which are bombings and shootings, are likely to rely on DNA or fingerprint evidence. The PSNI advises that the concept of DNA was unexplored during the majority of the Troubles and it is therefore likely that a relative lack of care was taken by terrorists (and criminals generally) with saliva, blood and other cellular material. Forensic Science Northern Ireland have similarly advised that in relation to older cases, even those offenders who were otherwise forensically aware would not have been taking 'DNA precautions' to avoid detection, as that technology was unknown at the time. The Department understands that developments in DNA profiling techniques over the last 30 years mean that exhibits previously determined as providing no forensic opportunities become potentially useful. This combined advice means that DNA will be particularly useful in relation to the cases examined by the ICRIR because in such cases there is a greater chance than in present day cases that offenders will not have guarded against leaving DNA traces on exhibits collected at crime scenes.

112. The Department considers that this evidence base is sufficient to justify some kind of exception to the new retention regime, and that the proposed retention regime in clause 30 can be justified as proportionate…'[315]

315 Northern Ireland Troubles (Legacy and Reconciliation) Bill: European Convention on Human Rights Memorandum.

**RECOMMENDATION 1**

In the event that this legacy snapshot is retained after the new Independent Commission for Reconciliation and Information Recovery has been established, the PSNI should obtain independent legal advice about the lawfulness of retention, disclosure and remedies.

### Current proposals

It is understood that any new provisions will not be introduced in the Assembly until at least 2023 (the absence of a functioning Assembly contributing to this delay). Currently the PSNI are having to operate a system that is unlawful with all the risks of litigation that this involves, the only permanent solution is for the Assembly to change the law.

In March 2022 the PSNI proposed to revisit the original proposal and to continue the work of the Biometric Ratification Committee on the basis of a Biometric Retention Service Instruction and this is now being implemented. The approach taken in the Service Instruction does not attempt to remedy the faults identified by the two ECtHR judgments referred to above but is much more limited in its aims. Individuals who request the deletion of their PACE biometrics will have their case considered by the PSNI's Biometric Ratification Committee, however this Committee will only consider early deletion in very restricted circumstances:

- Where the fingerprints and DNA were taken unlawfully;
- Where it has subsequently been decided that the alleged crime that resulted in the samples being taken did not occur – the example given is an arrest after a death but where subsequently it was discovered that the person died of natural causes;
- Where a person has a proven alibi and were eliminated from the enquiry following the arrest;
- Where the 'disposal' following the arrest was incorrect;
- Where the arrest was unlawful;
- Where the samples were taken as a result of mistaken identity;
- Where a judge recommends deletion; or
- Where another person is convicted for the offence and there is no possibility of their being more than one offender.[316]

Whilst these are all good reasons for deletion, they do not deal with the unlawfulness identified by the ECtHR.

316 PSNI's procedure is set out here https://www.psni.police.uk/biometric-deletion-requests

The PSNI should and can go further to ensure lawful retention and compliance with the ECHR. PACE, which provides the lawful basis for the taking and retention of samples and data, does not require retention, Article 64 of the Order only gives a power (and not a duty). The provision states samples 'may be retained.'[317] This gives the PSNI a discretion, a discretion which must be exercised lawfully, including only if compliant with the Human Rights Act, taking into account judgments of the ECtHR.[318] The current arrangements therefore appear to be unlawful and could open up the PSNI to expensive successful challenges and awards of compensation by, potentially, hundreds of people whose data continues to be held unlawfully (and was outlawed by the cases of S and Marper and Gaughran).[319]

Although a more lawful system would be more difficult to operate the ECtHR in Gaughran has set out the principles that need to apply (as above).

**RECOMMENDATION 2**

The PSNI obtain legal advice, which it should provide, in confidence, to the Policing Board's Human Rights Advisor so that it is able to re-write its Service Instruction, delete the unlawfully retained material, and ensure that, as far as possible, it complies with the two ECtHR cases.

317 Police and Criminal Evidence (Northern Ireland) Order 1989, Article 64(b).
318 Human Rights Act, section 2(1)(a).
319 For more details of the current retention and deletion arrangements see Service Instruction: Interim Service Instruction Biometric Retention 2022.

## ANNEX C

# BACKGROUND INFORMATION TO THE USE OF DRONES

The Home Office Code of Practice on Covert Surveillance and Property Interference states

> 'Where surveillance using airborne crafts or devices, for example helicopters or unmanned aircraft (colloquially known as 'drones'), is planned, the same considerations outlined in chapters 3 and 5 of this code should be made to determine whether a surveillance authorisation is appropriate. In considering whether the surveillance should be regarded as covert, account should be taken of the reduced visibility of a craft or device at altitude.)
>
> ***Example:*** *An unmanned aircraft deployed by a police force to monitor a subject of interest at a public demonstration is likely to require an authorisation for directed surveillance, as it is likely that private information will be obtained and those being observed are unaware it is taking place, regardless of whether the drone is marked as belonging to the police force. Unless sufficient steps have been taken to ensure that participants in the demonstration are aware that aerial surveillance will be taking place, such activity should be regarded as covert.'* [320]

The Human Rights Advisor has monitored the use of new drones and given feedback on the original draft Service Instruction which has now been published. There is also a Privacy Impact Assessment to go alongside the Service Instruction and the Human Rights Advisor will be reviewing its content in due course. However, there is no overarching policy governing the use of all the aerial platforms for surveillance.

Recommendation 4 in the Human Rights Annual Report 2020/21 stated:

> *'The PSNI Service Instruction should be extended to cover the use of all PSNI aircraft, should be published alongside the Privacy Impact Assessment and should set out, in summary, the Regulation of Investigatory Powers Act 2000 authorisation processes.'*

320 Revised Code of Practice, August 2018, para 318.

This recommendation was accepted by PSNI:

> 'The review of the Service Instruction is being progressed. Once the review has been completed, any relevant changes concerning the use of aircraft that impact on privacy will be made to the document. Post the review stage the Service Instruction and Privacy Impact will be subject to Service guidelines on the publication of official police documents to determine suitability for release in a public forum.'

And an update provided in December 2022:

> 'Following further review and internal consultation SOB has concluded that a Service Instruction is not the most appropriate mechanism for achieving the aims of the recommendation. The recommendation was grounded in data protection and privacy considerations for the use of Unmanned Aerial Systems (UAS) by the PSNI. That equipment is owned by and widely used by various departments across the entire organisation and as such a SI was developed and published to inform the wider organisation to ensure consistency and legal compliance of approach. The governance and authorisation processes for material gathered in the course of duties performed using other aerial assets (Fixed and Rotary Wing) sits solely in SOB. As such a series of standardised operating procedure documents have been developed to instruct the officers and staff in SOB, which address the issues raised in the recommendation.'[321]

321 Letter to the NIPB, January 2023

# ANNEX D

# EXTRACTS FROM THE IPCO INSPECTION REPORT

The Human Rights Advisor recently read the detailed report from IPCO's inspection of April 2022 and can disclose the following extracts from that report. Note that because some parts have been 'redacted' by PSNI the text appears a little broken and is sometimes a little difficult to understand:

### '4. Actions taken on previous inspection

Discharged – professional discussion has assured the inspection team…
continues to be managed and staffed by highly experienced officers…
the oversight and reassurance regime that has been created by…
continues to provide valuable assurance and learning to those engaged in covert operations…

### 5.2 Errors

an administrative error rather than a breach of the legislation…
not renewed in time… No contact or taskings took place during the unauthorised period…

### 5.3 Confidential Information

It is important that consideration always be given to the possible presence of LPP material in all cases…
legal advisors are both highly experienced and well versed in criminal law…confident in their ability to assess the presence of LPP material…
Investigating officers need to be aware that it is an area where professional legal guidance is usually required…
It was pleasing to note that there had been improvements made to applications and authorisations…
In general, applications were of a very good standard and benefited from the oversight and quality assurance of a number of persons…

Some operations can be very complex in nature, it is inevitable that the necessity and proportionality grounds can appear to be weakened progressively with the passage of time. The renewals tended to repeat the original grounds for the authorisation, rather than acknowledge the protracted nature of the deployment. A greater focus on what intelligence or evidential gaps remained, and how the continued use of the covert tactics could fill these, is recommended…

The applicant's assessment of collateral intrusion should describe in more detail what collateral intrusion has taken place, the future likelihood of it occurring, and the measures proposed to mitigate it. Such assessments should be bespoke to the nature of the activity and the tactics deployed…

While it was pleasing to note that cancellations were completed promptly…

Risk assessments clearly detailed the risks attached to each of the CHIS examined and were well maintained throughout the duration of the authorisation…

Very good practice was found in the submission and maintenance of policy logs detailing the regular reviews of the procedures attached to emergency contact and emergency extraction plans…this process is one the Force may wish to consider adopting as standard practice…

The oversight and governance of CHIS is extremely robust, and evidence of good practice was found in the frequent use of policy logs…

Contact sheets are very well maintained and demonstrate a detailed account of meetings with the CHIS, with an appropriate focus being placed on welfare…general good standards found…observations are made in relation to some of the cases examined…

Juvenile CHIS - No authorisations have been granted for the use of Juvenile sources within the inspection period…

PSNI has been subject of two previous standalone inspections on data assurance… The records should be clearly set out and supported by suitable reasoning for retention, review and disposal periods…

## 6 Conclusion

This inspection has demonstrated that PSNI has continued to maintain a high level of legislative compliance in respect of CHIS and Surveillance. The recommendation highlighted in the 2021 report has been discharged, albeit one area of non-compliance has emanated from this inspection, together with several observations highlighted as learning points to improve the already high standards found.'

# ANNEX E

# EXTRACTS FROM HRAR 2021/22 REGARDING CHIS

CHIS[322] may only be authorised for use in accordance with the RIPA and the IPA. Under RIPA a person is a CHIS if they establish or maintain a personal or other relationship with a person for the covert purpose of facilitating the doing of anything falling within: the covert use of a relationship to obtain information or to provide access to any information to another person; or the covert disclosure of information obtained by the use of such a relationship or as a consequence of the existence of such a relationship. Police officers and other personnel from law enforcement agencies can also be authorised as a CHIS (undercover police officers).

Special safeguards apply to the use or conduct of CHIS who are under 18 years. For example, the use or conduct of CHIS less than 16 years of age can never be authorised to give information against their parents or any person who has parental responsibility for them. In other cases, authorisations should not be granted unless special provisions are complied with.

Litigation by a number of NGOs raised questions about the lawfulness of CHIS being 'authorised' to commit criminal offences (see last year's Human Rights Annual Report for more details). As a result the Government in Westminster brought forward a Bill which was enacted by Parliament – the Covert Human Intelligence Sources (Criminal Conduct) Act 2021. Criminal Conduct Authorisations now allow MI5, police services (including the PSNI), and a range of other public authorities to authorise their agents and informants or CHIS to commit criminal offences, where it is necessary and give those people and those that made the authorisation complete immunity. In practice, the Act makes lawful an already widespread practice.

The Board suggested that the PSNI develop its own guidance on this authorisation process and that the Board have a role in approving this guidance. It was suggested that this guidance might help to reassure the public in Northern Ireland about both the procedures and the kinds of crimes that might be authorised. The guidance could impose specific restrictions or controls to try to deal with, at least some, of the important issues raised in Parliament during the passage of the Act but which were not dealt with sufficiently in that legislation. Careful guidance might also avoid the risk that PSNI violates human rights law (including the rights of innocent victims), limit

322 Sometimes referred to as 'informers'.

the use of children in committing "authorised crimes" and resolve some of the issues resulting from PSNI agents or others committing crimes in the Republic. The guidance (or at least parts of it) could also be subject to some kind of public consultation (including an equality impact assessment). The Human Rights Annual Report 2020/21 recommended:

'Recommendation 20:

> *Given the identification by many Parliamentarians of flaws in this Act and the concerns from the past of the use of CHIS and possible criminal offences, the PSNI should develop more detailed guidance to ensure human rights compliance.'*

The PSNI rejected that recommendation although internal guidance was drafted. However, the PSNI have been very open with the Human Rights Advisor on how it will use the new law and he attended a training seminar with the Criminal Conduct Authorisations (CCA) authorising officers and was able to ask questions and discuss the procedures and processes. In February 2022 he was shown the PSNI's internal draft guidance on CCAs and provided comments to try to strengthen the human rights principle that were set out. In September 2022 the Advisor was shown the final version.

## ANNEX F

# PSNI INTERNAL DRAFT GUIDANCE ON CRIMINAL CONDUCT AUTHORISATIONS

Note that because some parts have been 'redacted' by PSNI the text appears a little broken and difficult to understand:

**'PSNI Criminal Conduct Authorisations Guidance 2021 – includes redactions**
The use of Covert Human Intelligence Sources (CHIS) is a crucial tactic in preventing many crimes and safeguarding victims and the public from serious harm, including terrorism, drugs, firearms offences and child sexual exploitation.

The Criminal Conduct Act 2021 (the 2021 Act) provides an express power to authorise CHIS to participate in conduct which would otherwise constitute a criminal offence. This will only be authorised – **in very carefully managed circumstances**.

The new legislation is summarised below and the updated CHIS Codes of Practice 2021 outlines the process and consideration for the authorisation of Criminal Conduct and should be read in conjunction with this Policy.

Full implementation of the 2021 Act came into effect for the PSNI on 15 September 2021. This will necessitate the adoption of some transitional arrangements and a permanent change in how authorisations are granted for CHIS criminal participation.

As is the case from the inception of RIPA 2000 nearly 20 years ago, all CHIS authorisations **must be considered in terms of necessity and proportionality.** In addition, CHIS authorisations must be in compliance with overarching obligations under the European Convention on Human Rights (ECHR). These include the right to life, the absolute prohibition of torture and inhuman and degrading treatment and punishment and the prohibition of discrimination. Further details are set out at page 8 below.

CHIS will never be given unlimited authority to commit any and all crimes. A CCA must be detailed and specific about the conduct authorised and it must be accompanied by detailed risk assessments.

**The Act will not prevent prosecutors from considering a prosecution for any activity outside the authorised activity.**

The authorisations will have judicial oversight and will be overseen by the Investigatory Powers Commissioner (IPCO) who will be notified of any criminal conduct authorisation in writing as soon as practicable and always within 7 (seven) days…

### CoP 3.14

The following elements of proportionality should therefore be considered before granting a Criminal Conduct Authorisation (CCA).

- Whether what is sought to be achieved by the authorised conduct could reasonably be achieved by other conduct which would not constitute crime;
- Whether the criminal conduct to be authorised is part of efforts to prevent or detect more serious criminality;
- Whether the potential harm to the public interest from the proposed criminal conduct would be outweighed by the potential benefit to the public interest and that the potential benefit would be proportionate to the criminal conduct in question…

### CoP 6.45 – 6.49

6.45 Where a purported Criminal Conduct Authorisation does not meet the requirement the Part II of the 2000 Act, the conduct will not be rendered lawful by it.

6.46 Conduct that goes beyond what is authorised by Criminal Conduct Authorisation will also not be rendered lawful by it…

### Human Rights Considerations for CHIS Criminal Conduct Authorisations

The key aspects of compliance with Human Rights law are already built in to the Act and as previously highlighted section 29B(4), it sets out clearly that the granting of a CCA must be necessary (a) and proportionate to what is sought (b).

At section 29B(5) the grounds for necessity are set out, and at 29B(6) the important caveat in all covert deployments, that there was no less intrusive method available to achieve the same aim, in this case, activity that does not constitute a crime.

Section 29B(7) is very important, because it stipulates “that subsection (6) is without prejudice to the need to take into account other matters so far as they are relevant (for example, the requirements of the Human Rights Act 1998).

This means that human rights considerations must be taken into account and applied at all stages during consideration of a CCA. Authorisations should identify human rights issues and address them appropriately.

This is where you can add in some of the other considerations, for example;

**Article 2 ECHR** – duty to consider any real and immediate risk to life to any individual who is either subject to the CCA, or may be affected by it.

**Article 3 EHCR** – duty to protect individuals from torture and inhumane treatment, commonly associated with paramilitary style assault (PSA). A CCA cannot authorise conduct which could constitute torture or inhuman or degrading treatment or punishment. This is an absolute prohibition.

**Article 8 ECHR** – right to privacy and respect for family life. This is more commonly engaged in DSA, but may be relevant to CCA deployment.

**Articles 10 and 11 ECHR**– deal with freedom of expression and right to assembly and association. These rights are frequently engaged in protest situations, but are more likely to be infringed if the protest is stopped or prevented. Any consideration of Articles 10 and 11 would be very case specific, but are the nonetheless important.

**Article 14 ECHR** – freedom from discrimination, this would be engaged if an individual CCA or theme of CCAs amounted to a perceived targeting of any particular group without lawful purpose. Compliance with Article 14 can be achieved through proper consideration of all of the operational requirements and the necessity and proportionality tests.

Section 29C sets out very specific and detailed provisions regarding the tasking of juvenile CHIS. In addition to the significant legal protections within Section 29C, there are also considerations within the United Nations Convention on the Rights of the Child (UNCRC) which are vast. The Act was written with those protections in mind, but it is good to note that these may be relevant if we did in fact authorise in this manner.'

# ANNEX G

# LEGISLATION GOVERNING EXTRACTION FROM ELECTRONIC OR DIGITAL DEVICES

### Police, Crime, Sentencing and Courts Act 2022 Chapter 3 (Extraction of information from electronic devices)

The Police, Crime, Sentencing and Courts Act 2022 (PCSC) aimed to introduce a new statutory power enabling the police to obtain digital evidence from devices, providing safeguards are followed, and ensuring that only the relevant information is taken.[323]

The Act determines when an authorised person, such as law enforcement, may extract information:

> '(1) An authorised person may extract information stored on an electronic device from that device if—
> (a) a user of the device has voluntarily provided the device to an authorised person, and
> (b) that user has agreed to the extraction of information from the device by an authorised person'.[324]

These powers may only be used to prevent, detect, investigate, or prosecute crime, help to locate a missing person or protect a child or an at-risk adult from neglect or physical, mental, or emotional harm.[325] In the cases of children or an adult without capacity, their guardian can give consent. Furthermore, an authorised person must only exercise the Section 37 power for the purposes of preventing, detecting, investigating or prosecuting crime if they reasonably believe that information stored on the device is relevant to a reasonable line of enquiry.[326]

The 2022 Act does not specify under what circumstances law enforcement is entitled to seize electronic devices. Section 27 of the bill relies on voluntary provision of the device.[327] However, as will be explained in the section on Data Protection legislation,

323 https://www.gov.uk/government/publications/police-crime-sentencing-and-courts-bill-2021-factsheets/police-crime-sentencing-and-courts-bill-2021-data-extraction-factsheet
324 https://www.legislation.gov.uk/ukpga/2022/32/part/2/chapter/3/enacted
325 Ibid.
326 Section 37(2)(a) and Section 37(5)(a) and 37(5)(c) of the Act
327 Section 37 PCSC 2022

a person voluntarily handing over their phone does not constitute consent to their data being processed (in compliance with data protection law); and one does not include or presuppose the other.[328]

Interestingly, the Extraction of Information from Electronic Devices Code of Practice mentions that the 'voluntary provision in the PCSC Act does not equal 'consent' as defined under the Data Protection Act 2018'.[329]

The Code of Practice rightly states that if a less intrusive means of obtaining information are available, they must be considered, and used where reasonably practicable to ensure the extraction meets the test of strict necessity and proportionality.[330] A full extraction from a device will likely not meet the necessity and proportionality test.

### Criticism of the Act

There are a number of statutes that may be used to obtain stored communications for evidentiary purposes. Those most used by law enforcement in Northern Ireland include (but are not limited to):

- powers of search, seizure or production under the Police and Criminal Evidence (NI) Order 1989 (PACE)
- powers to search or obtain content under the Proceeds of Crime Act 2002;
- powers to search under The Firearms (NI) Order 2004, Protection of Children Act 1978, Theft Act 1968 and the Misuse of Drugs Act 1971;
- powers to search or examine under Schedule 7 of the Terrorism Act 2000.

In their May 2021 submission to the UN Joint Committee on Human Rights, Privacy international highlighted that the (then) bill 'demonstrates numerous failures to safeguard individuals' privacy. As a result, Privacy International argues that the Act in its' current form cannot comply with the right respect for private life under Article 8 ECHR'.[331] The powers go beyond mobile phones and refers to extracting undefined 'electronic devices'. Privacy International also highlights that the Act provides that 'electronic device' means any device on which information is capable of being stored electronically and any component of such a device. However, there is little information available on how or if police extract data from devices such as Amazon Echo, Google Home, Fitbit, connected toys, smart TVs and so on.

328 https://ico.org.uk/media/about-the-ico/documents/2617838/ico-report-on-mpe-in-england-and-wales-v1_1.pdf p.33

329 Extraction of Information from electronic devices: code of practice para 43, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1110883/E02802691_Electronic_Devices_Code_of_Practice_WEB.pdf

330 Ibid. para 78

331 Privacy International's Submission to The Joint Committee On Human Rights On The Draft Police, Crime, Sentencing And Courts Bill 2021 https://privacyinternational.org/sites/default/files/2021-06/PI%20Submission%20to%20JCHR%20re%20PCSC%20Bill_Final_0.pdf

Several organisations have voiced concerns that consent, or 'voluntary provision' should not be the basis for the legal measure granting powers to seize the device, nor agreement the basis for legal measures granting powers to extract data from electronic devices. Given the inherent power imbalance between the police and the user, the instances in which provision of a device will be truly voluntary is questionable, making it an unstable basis upon which to legally seize a device.[332] Similarly, the ICO's position on MPE is that the data a mobile phone holds cannot simply be 'given away' to a controller (in this case a law enforcement agency) by the device owner. Police forces need a good cause, based in law, to do this, as it includes data about other people and not just the device owner. Consequently, the practice of MPE needs controls that apply to protect the information rights and privacy of citizens. They need to apply regardless of whether a device is taken from a complainant, a witness, or a suspect.[333]

The Law Society has authored an extensive report on search warrants, published in 2020. The report argues that Search Warrants are a fundamental way to ensure against abuse or misuse of extraction powers. The legal framework that currently governs the search and seizure of electronic material was not designed with the ways in which electronic material is now accessed in mind. This means that the current law fails to appreciate the unique features of electronic material and digital investigations. As a result, the current law both inhibits criminal investigations and has significant privacy implications for those whose electronic devices are searched and seized.[334]

The report makes several recommendations which aim to ensure that the current framework governing search warrants operates effectively in the modern digital world so that evidence of criminality can be secured. At the same time, these recommendations aim to afford robust privacy protections in respect of the obtaining and subsequent treatment of electronic data.[335] However, these recommendations were not incorporated into the PCSC Act.

These shortcomings in the criminal justice legislation make it even more important for police forces to adhere to legislation on data protection, which will be discussed below.

332 https://privacyinternational.org/sites/default/files/2021-06/PI%20Submission%20to%20JCHR%20re%20PCSC%20Bill_Final_0.pdf

333 Information Commissioner's Office Mobile phone data extraction by police forces in England and Wales. An update on our findings (2021) https://ico.org.uk/media/about-the-ico/documents/2620093/ico-investigation-mpe-england-wales-202106.pdf p. 8

334 For example, current legislation such as PACE cannot be applied to data stored in the cloud, which most of us use on our mobile devices to back up data or simply extend a mobile phone's storage capability.

335 See Chapter 14 – 18, Law Commission Law Com No 396, Search Warrants (2020) https://s3-eu-west-2.amazonaws.com/lawcom-prod-storage-11jsxou24uy7q/uploads/2020/10/Search-warrants-report-grayscale-web-1.pdf

### Bater-James and Sultan Mohammed Judgment

Two otherwise unrelated cases[336] involving sexual assault were listed together and provided the Court of Appeal (Criminal Division) with an opportunity to consider various issues relating to the retention, inspection, copying, disclosure, and deletion of the electronic records held by prosecution witnesses. In the case of Sultan Mohammed v R, the police downloaded and copied the contents of the complainant's mobile phone, which amounted to 40,000 pages. They then used search terms to assist in identifying any messages that might indicate that the sexual intercourse had been consensual.[337]

The Court made clear that while the issues often arise in the context of complainants' telephones in sexual cases, the judgment is of potential relevance to a much wider range of circumstances The Court set out four issues of principle that will apply to all cases which involve digital communications, two of which are particularly relevant to the disclosure of digital communications:

1. Identifying the circumstances when it is necessary for investigators to seek details of a witness's digital communications, from whatever platform. The question is when does it become necessary to attempt to review a witness's digitally stored communications and when is it necessary to disclose digital communications to which the investigator has access?

   There is no obligation on investigators to seek to review a witness's digital material without good cause. Any such request must have a proper basis, i.e. that there are reasonable grounds to believe that it may reveal material relevant to the investigation or the likely issues at trial.[338]

2. When it is necessary, how should the review of the witness's electronic communications be conducted?

   The Court stated that a witness need not always surrender an electronic device. It recognised that such a loss could amount to an intrusion into the private life of the witness, regardless of the separate considerations of privacy as to the actual content.[339] The court highlighted that it may be possible to obtain the communications from the suspect's devices, or by reviewing the complainant's social media posts (on provision of a password) without the necessity to surrender the actual device.[340]

336 Bater-James and Sultan Mohammed v R (2020) EWCA Crim 790 (23 June 2020)
337 https://albionchambers.co.uk/disclosure-of-digital-records-the-key-to-the-sweet-cupboard-is-no-longer-left-in-the-keyhole/#_ftnref5
338 See also S. 3 (1) (a) of the Criminal Procedures and Investigation Act 1996
339 Bater-James and another v R (2020) EWCA Crim para 78
340 Ibid.

> However, assuming that a need to review the actual device is identified, the Court then indicated that a further important question to consider would be whether review of a discrete part of the digital record will suffice. This might involve focused questions or screen shots.[341]

### Data Protection Legislation

The Code of Practice provides guidance on the application of the powers in the PCSC Act. It correctly highlights that the powers must be exercised in accordance with the Human Rights Act 1998, the Equality Act 2010, the DPA 2018 and the UK General Data Protection Regulation (UK GDPR).[342]

### Data collection, processing and retention

'Processing', in relation to information, means an operation or set of operations which are performed on information, or on sets of information. This begins with collection, recording, organisation, structuring or storage[343].

According to the ICO, processing of personal data begins at the point that data stored on or accessed via the device is viewed or extracted. If no data is viewed or extracted from a device in the possession of the police, no processing has taken place.

The Chief Constable (or Commissioner) of each police force is registered as a Data Controller and must demonstrate compliance with the relevant legislation and oversight rules to lawfully process any data extracted from or accessed via a device.

#### *Taking possession of a device*

It is important to note that the consent an individual may give for the police to take possession of their phone is entirely distinct from the definition of 'consent' relevant to the extraction and viewing of any personal data from that phone under data protection law. There is a legal distinction between consenting to the police taking possession of the device (under common law) and Consent to the police processing the personal data contained on it (in compliance with data protection law); one does not include or presuppose the other.[344]

#### *Data processing*

Since police practitioners cannot be certain about the nature of the data before viewing it, they should proceed on the assumption that it is sensitive and should ensure that they are complying with Part 3 DPA 2018 requirements. As part of their accountability

341 Ibid. para 79
342 Home Office Extraction of Information from electronic devices: code of practice (2022) https://www.gov.uk/government/consultations/extraction-of-information-from-electronic-devices-code-of-practice/extraction-of-information-from-electronic-devices-code-of-practice-accessible
343 s3(4)(a) DPA 2018
344 https://ico.org.uk/media/about-the-ico/documents/2617838/ico-report-on-mpe-in-england-and-wales-v1_1.pdf p.33

obligations and to demonstrate compliance, police forces should carry out a Data Protection Impact Assessment (DPIA) when they design their data processing operations. This will offer evidence that they have:

- identified appropriate lawful bases for processing;
- respected the data protection principles by design;
- put in place an appropriate policy document about sensitive processing; and
- provided all required information to data subjects.

The DPIA must consider all the risks associated with the processing, including the potential impact of individuals' right to privacy, along with measures to treat these risks.

When a phone is taken into the possession of a force, officers must provide detailed information to the individual from whom the device is taken or acquired, containing:

- facts about what is being sought from the device;
- under what lawful basis; and
- what rights the individual has in respect of that processing.

Extraction may only be carried out by persons who are trained in extraction techniques and in accordance with the quality standards set out in the Forensic Science Regulator's Code of Practice[345].

*Retention of data and devices*

Regarding the retention of data, the PCSC Code of Practice states:

'Information which is extracted and deemed not relevant must be deleted unless there is a lawful basis to retain it. Any decisions regarding the retention or deletion of information should be considered in line with relevant disclosure guidelines.

Where excessive or other information has been obtained because it has not been possible to restrict the extraction to the relevant material due to technological reasons, or following review, information obtained is no longer deemed relevant, unless there is a lawful basis to retain it, it must be deleted.'[346]

The code of practice refers to the PPS Code for Prosecutors as the relevant guideline in Northern Ireland, however, this guideline does not refer to data retention and deletion at all.[347]

345 See Forensic Science Regulator Codes of Practice and Conduct FSR-C-107 [6], FSR-C-119 [7], FSR-C-134 [8], FSR-C-135 [9], available at: https://www.gov.uk/government/publications/forensic-science-providers-codes-of-practice-and-conduct-2021-issue-7

346 Para 138 & 139

347 https://www.ppsni.gov.uk/sites/ppsni/files/publications/PPS%20Code%20for%20Prosecutors.pdf

# ANNEX H

# SAMPLE DIGITAL PROCESSING NOTICE FAQ FOR SUSPECT

Police Service
of Northern Ireland

## DIGITAL PROCESSING NOTICE

### Suspect FAQ

This form contains important information. Please read the contents carefully and to the end of the document. If you have any questions, please ask the officer(s) you are in contact with for the purposes of the investigation.

### Why do the police need my device?

We have a legal duty to carry out all reasonable lines of enquiry when investigating a crime. We must look for all evidence that supports a case against a person as well as information or material that might undermine the case or support the suspected person.

Acquiring material from your device has been considered as a reasonable line of enquiry in this case – that means that there is an identifiable basis for believing that material is held on your device that is relevant to the investigation.

### Do I have to give my device to the police?

There are two ways the police can take possession of your device.

1. Use of a lawful power of seizure - The law permits us to seize your device from you in certain circumstances. The law also provides a power of search to locate the device in certain circumstances. The lawful powers used to search for and seize your device should be explained to you by the officer seizing it if practicable. You are not entitled to refuse when officers are exercising their powers of search and/or seizure lawfully and by doing so you may be committing further offences.

2. Taking the device with agreement - We may ask you voluntarily to provide us with your device, even when powers of seizure are available. If your agreement is forthcoming we will take possession of your device. This may occur, for example, if you are suspected of committing an offence but you are not being arrested.

Once we have possession of the device we will process the personal data on it in accordance with Part 3 of the Data Protection Act 2018. This section allows us to process personal data when it is required for a law enforcement purpose. There are conditions attached to this. As we expect to process sensitive personal data we will only acquire data from the device when it is 'strictly necessary' to do so for that law enforcement purpose. We also need to meet one of the conditions set out in Schedule 8 DPA 2018. The most likely conditions that will be met are:

- necessary for judicial and statutory purposes – for reasons of substantial public interest;
- necessary for the administration of justice;
- necessary for the safeguarding of children and of individuals at risk.

### How long will you keep my device for?

This will depend on the case circumstances. Often the officer seizing or taking possession of your device will not know this information. You will be provided with the details of the officer in the case, who will inform you of how long they expect to keep your device for.

### Will the police look at everything on my device?

Officers will look only at the material they deem relevant to the investigation.

Wherever possible we will acquire only the material we believe may be relevant, so that we can review it. The investigator will be required to record the material they are looking for and why they are looking for it before the extraction takes place. We may not give you this information as to do so may prejudice the investigation.

If technology does not allow us precisely to target only the relevant material, we may have to copy more material than we need. If this happens, the investigator will set clear parameters to satisfy the reasonable line of enquiry and review material only within those parameters. This could include reviewing within specific dates, focused enquiries using search terms or only reviewing particular message threads. The investigator will make a record of the parameters they have set and why they have set them. Material outside of these parameters will not be looked at.

### What will the police do with the material they take from my device? Who will they give it to?

If we make the decision to take no further action in your case then we will not share the material from it with anyone else, unless we identify an unrelated risk to any individual or we identify evidence of unrelated offences. We will tell you when we have done this unless to do would put anyone at risk or prejudice an ongoing investigation.

There may be exceptional circumstances when the information collected may be shared for other purposes. This might be in relation to civil matters before a family court or if you make a complaint about the handling of the investigation relating to your case, for example. Any sharing will be assessed in relation to necessity.

The decision to prosecute rests with the Public Prosecution Service. We will share relevant material with the prosecutor when submitting a file to the PPS and when a defendant has been charged or has been reported to the PPS for a decision to prosecute

Should you be charged with an offence, the material on your device will fall into one of three categories:

### Evidence

This is the material that the prosecution will use in court in order to prove the offence. This material will be served on you/your defence team by the prosecution.

### Unused material

This is material that is relevant to the investigation, any person being investigated or the surrounding circumstances of the case but not being relied upon to prove the offence in court. There is a duty on prosecutors to disclose material from this category to the defendant if it assists their defence or undermines the prosecution case.

### Non-relevant material

This is everything else that not in the first two categories. In some cases where we have been able precisely to target only the relevant material, there will not be anything in this category. Where we have had to acquire more than we need, we will delete this material wherever possible and as soon as possible. This includes material that has not been looked at because it was not within the parameters set by the officer.

There may be occasions when it is impossible to separate this material from material that falls into the first two categories. If this is the case, it will be dealt with as highlighted within PSNI Privacy Notice hyperlink

### How will my data be kept secure?

You may be particularly concerned about the security of any data which is copied and stored whilst the criminal investigation is ongoing. Here we briefly explain our commitment to keeping your data secure but you can find further details in the PSNI Privacy Notice referenced above, and in the Management of Police Information (MoPI) Authorised Professional Practice (APP) policy document issued by the College of Policing and available on their website (the link is included below).

Any data that is downloaded from your device is kept on PSNI secure databases. It will be handled, stored and retained securely in accordance with the provisions of the Management of Police Information (MoPI) APP and, in the case of sensitive data, it will not be stored for any longer than necessary.

Further details regarding privacy information, including your rights under data protection legislation, are set out in the PSNI Privacy Notice

The Management of Police Information (MoPI) APP can be found at the College of Policing website http://www.college.police.uk.

### Data Protection – what are my rights?

The Data Protection Act 2018 affords you certain rights. It also mandates that we tell you certain things, which we have set out below.

The Data Controller for the Police Service of Northern Ireland is the Chief Constable. The Data Protection Officer for the PSNI is zdataprotectionofficer@psni.police.uk

Under Section 45 Data Protection Act 2018, you are able to make data protection requests (also known as subject access requests or SARS). More information can be found on the ICO website

### Further questions or complaints

If you have any further questions in relation to the investigation please speak to the investigating officer in charge of your case.

If you have a complaint in respect of the investigation, you can contact the Police Ombudsman at policeombudsman.org or 02890 828600

If you have a complaint regarding how the police have handled your data from your device

device(s), you have the right to complain to the Information Commissioners Office, who are the UK's independent body set up to uphold information rights. They can be contacted through their website on https://ico.org.uk/make-a-complaint/ or 0303 123 1113.

# ANNEX I

# SAMPLE DIGITAL PROCESSING NOTICE

Police Service
of Northern Ireland

## DIGITAL PROCESSING NOTICE (DPNB)

**(Device taken from Suspect)**

*To be completed by the officer taking possession of the device. A separate form must be completed for each device. Provide a copy of this form and the Information Notice to the device owner once complete.*See note "A" on page 3 for exceptions.*

| | |
|---|---|
| **Crime Reference No:** | |

| | | | |
|---|---|---|---|
| **OIC Details** | | | |
| **Station / Department / Team** | | | |
| **Name:** | | **Service No:** | |
| **Device Details** | | | |
| **Exhibit Ref** | | | **Device Pattern Lock**<br><br>**Indicate beginning and end**<br>◯ ◯<br>◯ ◯<br>◯ ◯<br>◯ ◯<br>◯ ◯ |
| **Telephone No(s)** | | | |
| **Make of Device** | | **Model** | |
| **Memory Card Present** | **YES** ◯<br>**NO** ◯ | **No. of SIM Cards** | |
| **No. of memory cards** | | | |
| **IMEI No.** | | | |
| **SIM PIN Code** | | **Device Pass Code** | |
| **Alternative Lock Methods** | If alternative lock methods are present (e.g. fingerprint or iris) please ask suspect to disable | | |
| **Description of device condition (e.g. damage or faults, last used)** | | | |

| | | |
|---|---|---|
| **Device Security Protection** | **Not Protected** | ◯ |
| | **Subject refused to provide** | ◯ |
| | **Not requested – provide your rationale** | ◯ |

| Suspect Declaration | | | |
|---|---|---|---|
| Name: | | DOB: | |
| Address: | | | |
| Role: | | | |
| Declaration | I agree to provide my device to the Police for the purposes of extracting data. | | |
| Signature: | | | |
| Date and Time: | | Time | |
| Appropriate Adult Signature: (if applicable) | | | |

| Suspect refused to sign - Officer Declaration | |
|---|---|
| Name : | |
| Service Number: | |
| Date and time: | |
| Signature: | |

| I have reasonable grounds for believing that disclosure to the Suspect of (i) Lines of Enquiry, (ii) Providing a Copy of DPNb, and/or (iii) Providing updates regarding information extracted from the device is not appropriate.<br>*Provide the identifiable basis for how this belief has been formed.* |
|---|
| |

| *Note A - *If you complete this section to withhold investigative information from the suspect you should only provide copies of pages 1 and 2 of this form to the the Suspect A Suspect Information Form should still be provided.* | | | |
|---|---|---|---|
| **Name:** | | **Service No.** | |
| **Signature:** | | | |

**I consider that it is strictly necessary to extract only the following material from the device in order to progress this reasonable line of enquiry:**
*What material are you looking for and why is it strictly necessary to extract that material from the device? Be specific. For example: Whatsapp messages between person A and person B between set dates in which the offence is discussed. Explain why the material is strictly necessary in light of the reasonable lines of enquiry you have identified above.*

*The material I am seeking to extract pursuant to the reasonable line of enquiry is (provide relevant dates, or start and end dates, where possible):*

*The material is strictly necessary because:*

**Collateral Intrusion:**
*To what extent is there a risk of collateral intrusion and what steps, if any, have been taken or can be taken to mitigate this?*

*Collateral intrusion relates to the personal data of third parties on the device.*

| Suspect Declaration | | | |
|---|---|---|---|
| Name: | | DOB: | |
| Address: | | | |
| Role: | | | |
| Declaration | I agree to provide my device to the Police for the purposes of extracting data as set out in this form. I have been provided with a copy of DPNb and Information Notice | | |
| Signature: | | | |
| Date and Time: | | Time | |
| Appropriate Adult Signature: (if applicable) | | | |

| Officer Declaration | | | |
|---|---|---|---|
| I have/have not (DELETE AS APPROPRIATE) provided the victim/witness with a copy of this form and information notice. | | | |
| Name: | | | |
| Service Number: | | | |
| Date and time: | | Time | |
| Signature: | | | |

## AUTHORISATION FOR FORENSIC ANALYSIS

### This Must Be Authorised Prior To Extraction

*To be completed by the authorising Inspector*

| **Authority Required From** | **INSPECTOR** |
|---|---|
| **Is the device lawfully in police possessi?** | **YES** ◯ **/ NO** ◯<br><br>If no, detail below what action you have taken |
| **Has the device been interfered with or interrogated in any way? (By police)** | **YES** ◯ **/ NO** ◯<br><br>Explain: |

I have considered this request for mobile device extraction and the specific information requested as set out above.

I am satisfied that the extraction of this data is ***strictly necessary*** in order to pursue a reasonable line of enquiry having regard to ***the circumstances of this case***.

**YES** ◯ **/ NO** ◯

I have considered possible less intrusive methods of pursuing reasonable lines of enquiry such as and not limited to, the taking of screenshots of the device, the recording of a witness statement to evidence the material on the device, the completion of conclusive telecom enquiries to prove/disprove contact from parties, and the provision of the material on the device to the investigating officer via email or other electronic transfer.

**YES** ◯ **/ NO** ◯

I am satisfied that the extraction of material as outlined in this submission by the Investigating Officer, to pursue the reasonable lines of enquiry, is appropriate in this instance

**YES** ◯ **/ NO** ◯

I the request.

| **Name** | | **Signature** | |
|---|---|---|---|
| **Date Authorised** | | **Time Authorised** | |

# ANNEX J:

# LIST OF PSNI DATA PROTECTION IMPACT ASSESSMENTS

| | |
|---|---|
| Jun-2018 | Sickness and duty adjustments |
| Jul-2018 | HR Recruitment Website |
| Sep-2018 | Firearms Licensing Website |
| Sep-2018 | Sickness and duty adjustments |
| Sep-2018 | Attendance Management |
| Sep-2018 | Mediation on SAPs |
| Sep-2018 | PUMA replacement |
| Oct-2018 | Police College Partnership with Uni |
| Oct-2018 | Anti Corruption Unit Risk assessment template |
| Oct-2019 | ANPR |
| Oct-2019 | FSNI Service |
| Mar-2019 | Interpreting Service |
| Mar-2019 | Prum Sharing |
| Feb-2020 | Belfast City Crime Watch |
| Feb-2020 | OHW Sessional Mental Health |
| Jun-2020 | PSNI Drones |
| Jun-2020 | OHW IHR DPIA |
| Jun-2020 | Recording Victim and Witness Statements Over Telephone and Using Box |
| Jun-2020 | In-Service Vetting |
| Jun-2020 | Covid Testing |
| Jun-2020 | Covid Tracking and Tracing |
| Jun-2020 | OHW Service Review |
| Jul-2020 | Recruitment and Selection |

### Services for Student Officers

| | |
|---|---|
| Jul-2020 | Covid Travel Regs with Home Office |
| Sep-2020 | Community Monitoring |
| Jun-2021 | MS Teams |
| Feb-2021 | Mobile Phone Extraction |
| Sep-2021 | Corporate Information Branch Review |
| Sep-2021 | Police Staff Website |
| Sep-2021 | NPCC Cryptocurrency Service |
| Oct-2021 | MOPI ToR and DPIA |
| Oct-2021 | UKSV DPIA |
| Dec-2021 | PSNI Service Medal |
| Jan-2022 | PSNI Integrated Vehicle Technology Solution |
| Jan-2022 | Dept of Infrastructure Transport Regulation Unit |
| Apr-2022 | Traffic Jam |
| Apr-2022 | Op Driver |
| Apr-2022 | Hate Crime Advocacy |
| Apr-2022 | HSCT SAIs |
| May-2022 | Voice to Text Service |
| May-2022 | Traffic Jam |
| Jun-2022 | Ileap for Origin FDS |
| Jul-2022 | Synalogik Data Matching |
| Aug-2022 | SOLA (Sexual Offence Legal Advisors Service) |
| Sep-2022 | Counter Corruption Board |
| Oct-2022 | Air Support Unit DPIA review |
| Oct-2022 | UKUSDAA and IPA data sharing |
| Oct-2022 | Substance Abuse Testing Service |
| Nov-2022 | Google Meets UKSV DPIA |
| Dec-2022 | Complex Lives Partnership |

| | |
|---|---|
| Dec-2022 | Vehicle Recovery Service |
| Dec-2022 | Migrant Help Service |
| Dec-2022 | PSD Review Panel |
| Jan-2023 | Rayuela Int Research Project |
| Jan-2023 | Facial Recognition / Matching CRS |
| Jan-2023 | Cultural Audit by 3rd Party |
| Jan-2023 | Historical Data Wash (National) |

# GLOSSARY

| | |
|---|---|
| **AI** | Artificial Intelligence |
| **ACRO** | Criminal Records Office |
| **ANPR** | Automated Numberplate Recognition |
| **APP** | Authorised Professional Practice |
| **BWV** | Body worn video |
| **CCA** | Criminal Conduct Authorisation |
| **CJA** | Criminal Justice (Northern Ireland) Act 2013 |
| **CJINI** | Criminal Justice Inspectorate Northern Ireland |
| **CHIS** | Covert Human Intelligence Source |
| **CPT** | Covert Policing Team |
| **CoP** | College of Policing |
| **CRS** | Community Rescue Service |
| **CSU** | Cyber Support Unit |
| **DoJ** | Department of Justice |
| **DNA** | Deoxyribonucleic acid |
| **DPA** | Data Protection Act 2018 |
| **DPIA** | Data Protection Impact Assessment |
| **DPN** | Digital Processing Notice |
| **DPO** | Data Protection Officer |
| **DVLA** | Driver and Vehicle Licensing Agency |
| **ECHR** | The European Convention of Human Rights |
| **ECtHR** | The European Court of Human Rights |
| **ECRIS** | European Criminal Records Information System |
| **EIS** | European Information System |

| | |
|---|---|
| **FRT** | Facial Recognition Technology |
| **GDPR** | European General Data Protection Regulation |
| **ICCPR** | International Covenant on Civil and Political Rights |
| **ICO** | Information Commissioner's Office |
| **IPCO** | Investigatory Powers Commissioner's Office |
| **IPT** | Investigatory Powers Tribunal |
| **LFR** | Live Facial Recognition |
| **MoU** | Memorandum of Understanding |
| **MPE** | Mobile phone extraction |
| **NGO** | Non-governmental organisation |
| **NIO** | Northern Ireland Office |
| **NIPB** | Northern Ireland Policing Board |
| **NLEDS** | National Law Enforcement Data Service |
| **NPCC** | National Police Chiefs' Council |
| **OCDA** | Office for Communications Data Authorisations |
| **PACE** | Police and Criminal Evidence Act 1984<br>Police and Criminal Evidence (NI) Order 1989 |
| **PCSC** | Police, Crime, Sentencing, and Courts Act 2022 |
| **PNC** | Police National Computer |
| **PND** | Police National Database |
| **PPS** | Public Prosecution Service |
| **RIPA** | Regulation of Investigatory Powers Act |
| **SIS** | Schengen Information System |


Northern Ireland PolicingBoard

**Northern Ireland Policing Board**
James House
Block D, 2 – 4 Cromac Avenue
The Gasworks
Belfast BT7 2JA

**028 9040 8500**
**information@nipolicingboard.org.uk**
**www.nipolicingboard.org.uk**
**policingboard**
**@nipolicingboard**
**nipolicingboard**
**Northernirelandpolicingboard**

**DOCUMENT TITLE**

Human Rights Review of Privacy and Policing

**ONLINE FORMAT**

This document is available in PDF format from our website.

**PUBLISHED JULY 2023**

This document may also be made available upon request in alternative formats or languages. Requests should be made to the Northern Ireland Policing Board.

**DISCLAIMER**