Police Service
of Northern Ireland

Chief Constable's Report
to the Northern Ireland
Policing Board

Covert Powers in Relation to Journalists and Lawyers

we care
we listen
we act

Contents

Executive Summary

Executive Summary

During 2023 public and stakeholder concern was building in response to media coverage of reports of inappropriate use, by the Police Service of Northern Ireland, of covert powers against journalists and latterly lawyers. In response to this concern, the Northern Ireland Policing Board requested the Chief Constable to provide a report giving reassurance that the powers were being used appropriately, lawfully, proportionately and only where necessary, so as to maintain confidence in the Police Service. In April 2024 the Chief Constable provided an interim report and briefed the Policing Board on the issue. It was then agreed that a further detailed report would be provided, which would be publicly available. This is that report.

Police have a wide range of covert powers, as are detailed throughout this report, but public concern and commentary has focused on two principal aspects; communications data and the additional protection that the law provides, and society expects, for people in certain professions handling confidential material. It is the interplay of these two aspects that most concerns the public; namely whether the Police Service are striking the appropriate balance when accessing communications data for those people whose communications are particularly confidential, due to the nature of the work they do.
It is clear though, that much of the commentary provided to date has not accurately represented the powers police use in respect of our calls, emails, texts and our social media usage. The main power police use is for communications data only; simply put that is the who, where, when and how of our communication but **it is not** what was said, written or spoken.

> ***For example:***
> *Mobile Phone Number A (connected to Person A) sent a text message to Mobile Phone Number B (connected to Person B) at 12:34hrs on 5/6/24 and approximate locations of both mobile phones when they respectively sent / received the message.*

This is typically similar to what many people would recognise from mobile phone itemised billing data with additional datasets for policing purposes. The Police Service make around 8,500 communication data requests annually for a range of criminal offences. The most frequently investigated crimes using these powers are drugs related and since 2011 there have been in excess of 110,000 such requests. We also use communications data requests to assist in locating missing persons where someone's life is at risk. Over the last decade, as the way we

communicate has become more complex and diverse, the number of communications data requests has increased, as has their importance to our investigations. This is a trend we have seen across policing, reflecting increasingly digitally enabled crime.

From 2011 to 2019 these authorisations required the approval of a senior police officer, unconnected with the investigation, and trained to independently apply the legal and human rights principles relevant to the authorisation. Depending on the type of data sought, this was either an Inspector or Superintendent in the Police Service of Northern Ireland. Authorisations can only be granted for specific purposes. In 2019 the Office of Communications Data Authorisations took over this role and currently most authorisations in policing are for the purpose of prevention and detection of crime or to prevent disorder.

Requests for communications data for journalists have the potential to engage the protection afforded to them not to disclose their journalistic sources. This protection is provided for in UK domestic law and is reinforced by a number of decisions made by the European Court of Human Rights. However that protection is not absolute. It does not protect a public official or person who discloses documents or information without authorisation. Those individuals can be subject to misconduct and in some cases criminal sanctions.

In 2014 there was similar public concern in England and Wales following reports that the Metropolitan Police and Kent Police had used powers to obtain the communications data of journalists inappropriately in investigations involving Andrew Mitchell and Chris Huhne. In response the Interception of Communications Commissioner, the Right Honourable Sir Paul Kennedy, conducted a UK-wide inquiry, which included the Police Service of Northern Ireland, on the use of the powers to identify journalistic sources. The Commissioner found that police services had applied the relevant legal Code of Practice at the time, but that the Code did not provide sufficient protection or safeguards for journalistic sources. This was not a unique issue to PSNI, it affected the whole of the UK and all of law enforcement. As a result the UK Government introduced a new Code of Practice in March 2015 which required that a judge approve every instance that police sought to obtain communications data to identify a journalist's source. Police Inspectors and Superintendents continued to authorise all other applications. This was intended to be an interim step until new legislation could deal with the issue.

New legislation was introduced in 2016 and became operational in February 2019 with the creation of a new organisation, the Office of Communications Data Authorities (OCDA). This body took responsibility from police services across the UK, including the PSNI, for authorising almost all communications data applications. Where police seek to identify a journalist's source, approval of a judicial commissioner is now required within OCDA. On 1st March 2024 OCDA merged with the Investigatory Powers Commissioners Office.

From 1st January 2011 to 31st March 2024 there were 323 applications for communications data relating to journalists who were victims, suspects or witnesses to crime. Of those, 10 sought to identify a journalistic source using covert powers. The remainder of the applications did not seek to identify a journalist's source and their profession may have been entirely unrelated to the request.

Whilst lawyers' communications also receive special protection both in UK domestic law and through the case law of the European Court of Human Rights, it is of a different nature, primarily , but not exclusively, focusing on the confidentiality of the correspondence. In that way, whilst lawyers are a sensitive profession for communications data, the issue is more relevant to other covert powers which deal with what is said or written in a communication.

From 1st January 2011 to 31st March 2024 there were 500 applications for communications data related to lawyers who were victims, suspects or witnesses to crime.

In many instances the Police Service sought communications data in similar circumstances to those identified in the Inquiry conducted by Sir Paul Kennedy; that is where there were suspicions that police officers or police staff were inappropriately disclosing information or documents to journalists. This can be a crime on the part of the officers and staff, and will very often lead to misconduct proceedings. Such behaviour is often identified through lawful business monitoring by the Police Service, involving the use of no covert powers at all, but simply the checking of calls made from police phones to the contact numbers made available by journalists. This has recently been mischaracterised as a 'defensive operation' directed towards journalists. It is not. It is normal practice for most regulated professions, and many businesses to check that their staff are not making inappropriate calls from work phones. It is, unfortunately, a necessary tactic to ensure the high standards we set for our officers and the importance we afford to protecting data and information with which we are entrusted, as the public would expect. Occasionally those individuals are found to have been in contact with journalists or others in sensitive professions who deal with confidential information.

The Police Service also have a range of other surveillance powers available, which are tightly regulated and highly sensitive. The powers are detailed briefly within this report. The powers require increasingly senior levels of authorisation, proportionate to the intrusiveness of the power, beginning with Superintendents and ultimately requiring the approval of the Secretary of State for Northern Ireland. None of these other covert conduct powers available to the Police Service of Northern Ireland have been authorised from 1st January 2011 to 31st March 2024 where journalistic material or legal professional privilege material was sought.

The Chief Constable has a deep personal and professional commitment to ensuring that human rights principles are respected and upheld by the Police Service of Northern Ireland. These principles of proportionality, necessity, lawfulness and consideration of collateral intrusion are embedded in how the Police Service use the powers available to them. Whilst recognising the independent statutory bodies of the Investigatory Powers Commissioner's Office and the Investigatory Powers Tribunal, he also recognises the significant role of the Policing Board in ensuring public confidence and accountability in the use of these powers. In line with the Chief Constable's duties to report to the Policing Board and to further assure the public, stakeholders and partners on these issues the Chief Constable has developed, in addition to the publication of this report, an assurance plan to be led by Mr Angus McCullough KC acting as an independent special reviewer. Mr McCullough is a senior barrister with extensive experience as a special advocate, a role which involves analysing, probing, and challenging closed material, as well as seeking as much openness in legal proceedings as is consistent with the legitimate public interest in restricting disclosure. He will independently seek to evaluate the concerns of the public and stakeholders. His work will be supported by a wide-ranging steering group of experts. As reviewer, Mr McCullough will have unrestricted access to Police Service records and personnel to do his work but will not encroach on issues under consideration in the current IPT proceedings. This review does not affect the existing statutory regime for authorisation and oversight of investigatory powers, in particular by the Investigatory Powers Commissioner and his office.

The central public concern has been that there was widespread, and unjustified, surveillance of journalists and to a lesser extent lawyers. Without pre-judging the outcome of the independent review, the Police Service believes that this is not made out by the facts. The most frequently used power in respect of journalists was the acquisition of communications data, where journalists accounted for less than 0.5% of authorisations of all types. Those authorisations to identify a journalist's source accounted for only 10 authorisations since 2011, from a total of 110,000 made by the Police Service of Northern Ireland. Those applications sought to identify police officers and staff who were disclosing information and documents without authorisation. It was suspected that in doing so those individuals were putting others at risk and were potentially committing criminal and misconduct offences.

1: Introduction

1.1
By correspondence dated 15th Sept 2023 the Chair of the Northern Ireland Policing Board (NIPB), Ms Deirdre Toner requested 'any information held by the Police Service of Northern Ireland (PSNI) concerning any applications or authorisations for communications data or other surveillance powers under Regulation of Investigatory Powers Act 2000 (the 2000 Act) or the Investigatory Powers Act 2016 (the 2016) of any person known or suspected to be a journalist or a lawyer or, any person who has sought to obtain journalistic material from the PSNI during the years 2011 to 2015.'

1.2
This request was subsequently extended to the period ending December 2018 and on 11th April 2024 the Chief Constable agreed to provide a fuller report addressing the issues herein which will cover the period ending March 2024. This will now be referred to as the reporting period and for clarity is the period from 1st January 2011 to 31st March 2024.

1.3
In addition there has been considerable public and media narrative of late, suggesting the Chief Constable should address three particular areas of concern:

i. Firstly, to provide additional information and assurances regarding media reported activity undertaken by the PSNI, as reported in relation to ongoing Investigatory Powers Tribunal (IPT) proceedings;

ii. Secondly, to provide additional information and assurances as to what other activity the PSNI undertook over similar time periods that is not being examined by the IPT; and

iii. Finally, to provide assurance regarding the current practices of the PSNI in relation to surveillance of journalists, lawyers or other sensitive professions.

1.4
As explained at paragraph 5.6 the Investigatory Powers Tribunal (IPT) is an independent statutory court with jurisdiction over point (i). Usually the Chief Constable would make no comment on on-going proceedings until their conclusion. However, in this instance inaccurate reporting has given rise to serious public concern regarding the use of police powers. This has required the Chief Constable to address the concerns directly. These concerns are addressed in full in Appendix A, a copy of which has been provided to the Minister for Justice.

1.5
It is in the context of serious public concern that the Chief Constable has agreed to provide a detailed report to the Policing Board covering the use of covert powers, on an exceptional basis including detailed

statistical data to the Policing Board, intended to also address points (ii) and (iii) above. However, the ability to report on an on-going basis, in this area of policing powers, would be heavily restricted in the future by statutory constraints placed upon the Chief Constable. The extended reporting period used in this document mitigates the risk of identification of individual cases and therefore facilitates more detail than would be the case for a report covering a shorter time period, such as an annual report, for example. It should be noted though, that the Investigatory Powers Commissioner's Office (IPCO) carries out annual inspections of this nature as a matter of course. IPCO Annual UK reports are publicly available and the NIPB Human Rights Advisor has been directly engaged in the last two inspections. The latest of these was carried out in April and May of this year. Requestors of similar information in the future will be directed to available IPCO reports.

Legal, Policy Constraints

1.6
There are a number of express statutory provisions which limit disclosure of information concerning applications or authorisations under the Regulation of Investigatory Powers Act 2000 (the 2000 Act) and the Investigatory Powers Act 2016 (the 2016 Act). The provisions impose a statutory duty, now under Section 57 of the 2016 Act, on a category of persons, not to disclose information contained within section 57(4). For current purposes the Chief Constable, Deputy Chief Constable, all police officers and police staff members are subject to this duty.

1.7
The information not to be disclosed includes the existence or contents of any warrants for interception of communications, details of the issuance or renewal or modification of the warrant, any steps taken in pursuance of the warrant and any material obtained as a result of the warrant.

1.8
This position is further entrenched by section 59 of the 2016 Act which creates a criminal offence for unauthorised disclosure. Section 58 creates a category of excepted disclosures, however it does not, as currently framed, include disclosure to the Northern Ireland Policing Board. Notwithstanding these provisions, the Chief Constable has determined that, given the extent of the reporting period and the aggregation of total numbers of authorisations, approvals and warrants issued, his duty under section 57 has been met.

1.9
On 7th May 2024 Mr John Wadham, Human Rights Legal Advisor to the Northern Ireland Policing Board, reviewed all applications for communications data which touched

on the issue of journalistic sources, to further reassure the Policing Board of the compliance with the statutory scheme. This included a review of the redacted applications, the basis of the application, the data sought and the relevant periods for which data was sought.

1.10
Turning therefore to the areas that can be addressed without prejudice or breach of any statutory duty, covert powers and surveillance powers relevant to journalists and lawyers can be categorised under three domains:

- **Communications Data** – which relates to how the Police Service of Northern Ireland obtain the who, where, when and how of a communication but not its content, i.e. not what was said, written or spoken.

- **Conduct** – which relates to how the Police Service of Northern Ireland use the covert tactics powers of covert human intelligence sources, directed surveillance, intrusive surveillance and property interference.

- **Content** – which relates to the circumstances in which the Police Service of Northern Ireland obtain the content of a communication whilst being transmitted, and interfere with a person's equipment to obtain information or communication on that equipment.

1.11
A full explanation of these terms along with examples is available on the IPCO website: **ipco.org.uk/investigatory-powers/the-powers/.**

2: Communications Data

2.1
Authorisations for communications data is the most used power under both the 2000 and 2016 Acts, accounting for in excess of 90% of all authorisations, approvals or considerations[1] across the UK. The primary legal basis to access communication data for journalists and lawyers for much of the time between 2011 and 2019, on the rare occasions it was required, was Chapter 2 of Part 1 of the 2000 Act. The Act however, must be read in conjunction with and alongside relevant human rights standards; principally the European Convention on Human Rights[2]

Chapter 2 of Part 1 2000 Act

2.2
There are strict legal rules on who can obtain communications data and the circumstances in which the data can be accessed from a communication service provider (CSP). Communications data in practical terms is defined as the **who, when** and **where** of a communication, but not what was said[3] for example:

> *Mobile Phone Number A (connected to Person A) sent a text message to Mobile Phone Number B (connected to Person B) at 12:34hrs on 5/6/24 with approximate locations of both mobile phones given when they respectively sent / received the message.*

2.3
Importantly communications data **does not** include the content of the communication, i.e. what was said or contained within the communication. The content of a communication is dealt with under a separate process and for the purposes of this report is referred to as content data under a separate authorisation process.

Number of Applications and Authorisations

2.4
When considering the communication data authorisations or applications, the common metric of 'item of data' is used to provide meaningful comparison within statistics. Since 2015 the Interception of Communications Commissioner (IOCCO) and now Investigatory Powers Commissioner's Office (IPCO) have used this metric to allow meaningful annual comparisons to be drawn that align with national standards on statistics. An item of data is a request on a single communication address or telephone number or other communication identifier. For example, 30 days of incoming and outgoing call data in relation to a mobile phone would be counted as one item of data.

[1] *See IPCO Annual Report 2022, Tables 19.1 & 19.2*
[2] *The Interception of Communications Commissioner succinctly set out the legal framework which was in operation for the period 2011-15 in his report on accessing journalistic sources in 2015.*
[3] *Communications data is defined within section 261(5) of the Investigatory Powers Act 2016*

Equally, a request for the details of a subscriber to a communications service would be counted as one item of data. Each item of data requires authorisation, with each authorisation obtained by means of an application. However an application may seek more than one authorisation for more than one item of data. The previous report referred to the number of applications, whereas this report[4] will refer to the number of authorisations and applications. It is also important to note not all applications are authorised; some applications are not authorised when assessed against the relevant legal statutory test.

2.5

In common with other UK police services the Police Service of Northern Ireland saw rising numbers of authorisations for communications data between 2012 and 2021. The introduction of combined authorisations in 2022 substantially changed the process. Whilst duplication in the application stage was reduced, the overall numbers of items of data received as a result continues to increase year on year, as does the number of applications required, given the ever-developing complexity of investigations and diversity of communication sources used by the public today. Combined authorisations are a small measure to mitigate this rise in demand, making the process more efficient by allowing investigators to see authorisations for both subscribers and traffic data in a single rather than multiple applications.

2.6

To date IPCO has not commented on the national trends of combined authorisations, however we expect the impact on the Police Service of Northern Ireland to have been mirrored elsewhere. The below table outlines the number of authorisations for all communication data (not just journalists or lawyers) during the reporting period. In total there were 111,474 authorisations for communication data within the reporting period. On average each year there were 8574 authorisations between 2011 and 2023.

Year	Authorisations
2011	**4490**
2012	**4076**
2013	**6222**
2014	**8067**
2015	**8105**
2016	**9272**
2017	**9777**
2018	**10217**
2019	**10513**
2020	**11176**
2021	**11004**
2022	**9188**
2023	**9367**

[4] *A Briefing note for Northern Ireland Policing Board (NIPB) Members related to the covert surveillance of journalists and lawyers regarding the use of Communications Data and other Surveillance powers, dated 7/04/2024.*

Authorisation for Communication Data

2.7
Where an officer investigating a criminal offence believes it is necessary to obtain communications data, they can apply via a specific process to a designated person. This process ensures that decision making on the authorisations for communications data is separate from the investigation and applies the appropriate statutory test; considering the necessity, proportionality and lawfulness of the application. Applications are made via an audited computer system which enabled a robust inspection regime by the Interception of Communications Commissioner up until 2017 and IPCO thereafter.

2.8
Whilst different public authorities have different arrangements for designated persons, in the Police Service of Northern Ireland designated persons are all Inspectors and Superintendents who have been identified and appropriately trained to fulfil this role. The roles and responsibilities of designated Inspectors and Superintendents are dealt with in Section 3 of the Code of Practice on the Acquisition and Disclosure of Communications Data. There are two versions of the Code which applied during the reporting period, the 2007 Code applied during the period 2007- March 2015, hereafter the 2007 Code. As will be discussed later, in paragraph 2.49 below, this Code was superseded by a new code in March 2015, hereafter the 2015 Code. The below section deals with the 2007 Code.

2.9
The designated Inspectors and Superintendents are required to:

- Consider the application and if they believe it necessary and proportionate in the specific circumstances, grant the authorisation or notice;
- Have a working knowledge of human rights principles, specifically necessity and proportionality and how they apply to Chapter 2 and the Code;
- Not give authorisations in respect of any investigation or operation in which they are directly involved with except in cases of urgency or security.

2.10
Officers are required to undergo specialist national training which lasts for seven days, covering areas including proportionality, necessity, collateral intrusion and risk management. Officers undergo refresher training every three years to ensure they remain skilled and competent in the area. This is supported by a period of shadowing an officer experienced in authorising the powers.

2.11
When an authorisation has been given by a designated Inspector or Superintendent, a single point of contact within the Police Service of Northern Ireland is accredited to obtain the communications data from the communications service provider. Additionally a Senior Responsible Officer is appointed to ensure the integrity of the processes and systems as a whole, and ensure compliance with Chapter 2 and the Code. At all material times the Senior Responsible Officer in the Police Service of Northern Ireland was a Detective Superintendent.

Test to be Applied by Designated Inspectors or Superintendents

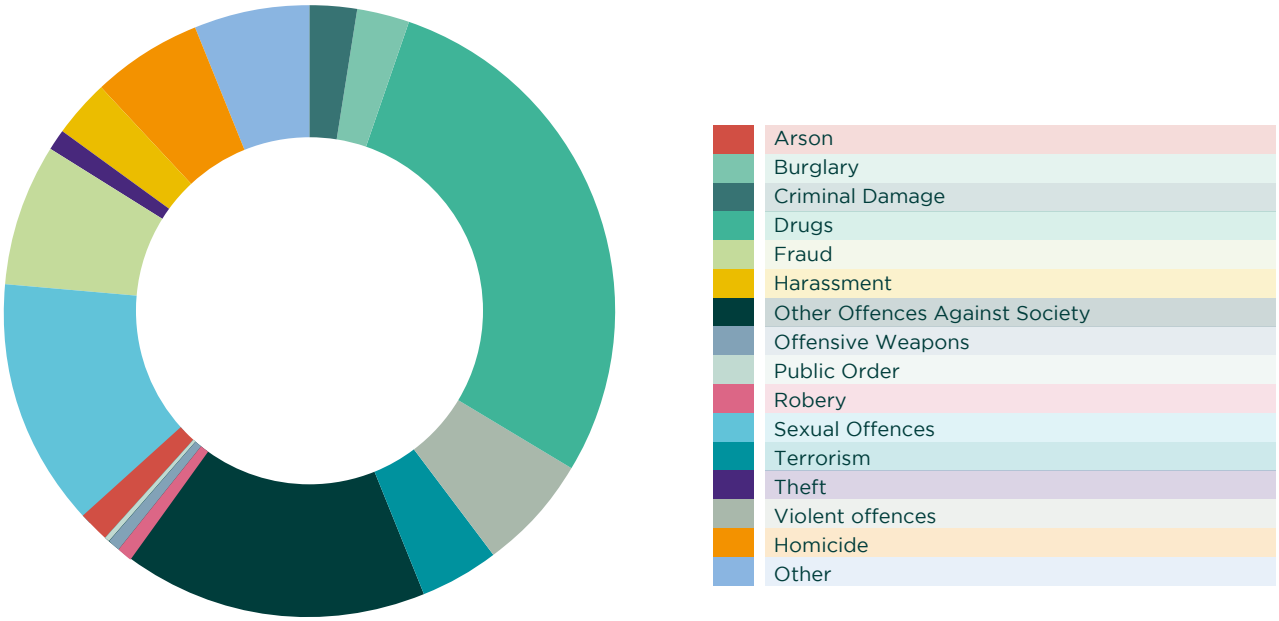
2.12
The test to be applied by the designated Inspector or Superintendent, is set out in section 22(2) of the 2000 Act. This is whether obtaining communications data is necessary for one of eight prescribed purposes, however in policing terms there are overwhelmingly two purposes most frequently used:

1. For the purposes of preventing or detecting crime or of preventing disorder;
2. For the purpose, in an emergency, of preventing death or injury or any damage to a person's physical or mental health, or of mitigating any injury to a person's physical or mental health.

2.13
The statutory test therefore specifically considers the issue of necessity in the authorisation process. It is also important to note in the context of communications data that the 2000 Act does not restrict authorisations to serious crime as defined in s81(3); it only requires that it is necessary for the purposes of preventing and detecting crime generally, which can be applied to a much wider range of investigations such as drugs offences, sexual offences and violent offences. However it also assists in cases when someone's life is in danger or a person is at significant risk of harm to themselves; a core purpose of policing.

2.14
The below chart outlines the range of offences for which communication data was authorised within the reporting period.

Investigations For Which Communication Data Was Authorised In 2023



Code of Practice

2.15
The test provided in section 22(2) is supported by the 2007 Code of Practice. Section 72 of the 2000 Act deals with the effect of the Code, requiring that designated Inspectors and Superintendents are required to have regard to the Code, that the Codes are admissible in evidence for criminal and civil proceedings, and failure to follow the Code does not render the designated Inspector or Superintendent personally liable to criminal or civil proceedings.

Process for Authorisations

2.16
The Police Service applies different levels of authorisations for different types of communication data. In broad terms there are three types of communication data:

Type of Data	Description	Practical Example	Designated Persons
Traffic data	Data that may be attached to a communication for the purpose of transmitting it and could appear to identify the sender and recipient of the communication, the location from which and the time at which it was sent. Under the 2016 Act this is now called 'Event data'.	Approximate location of the phone when calls are made or received, time at which the call was made.	Superintendent
Service use information	Data relating to the use made by any person of a communication service. Under the 2016 Act this is now called 'Entity data'.	Itemised billing for a mobile or landline phone service	Superintendent
Subscriber information[5]	Data in relation to a customer and may be the kind of information which a customer typically provides when they sign up to use a service. Under the 2016 Act this is now called 'Event data'.	Registered details with an email service provider	Inspector

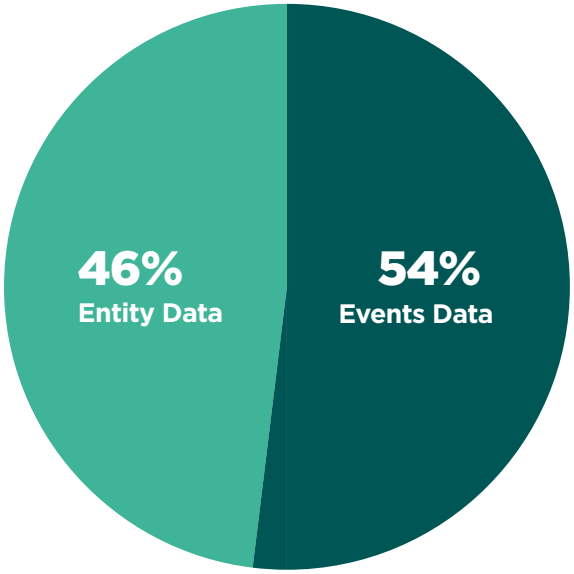
[5] This is commonly referred to as subscriber checks however this equally applies to enquiries to identify the user of an email account or social media account.

2.17

As a result of the introduction of combined authorisations in 2022 the Police Service of Northern Ireland introduced revised IT to assist with the process for obtaining communication data. As a result of this revision it is no longer possible to provide a breakdown of the relative number of authorisations for traffic data, service use information and subscriber information with a reasonable level of accuracy. IPCO commented on this change in their 2022 annual report, noting that, notwithstanding the issue, their confidence in the authorities was not reduced. The most recent data available to the Police Service of Northern Ireland shows for all items of communications data received, that 46% related to entity data (which previously would have broadly aligned to service use and subscriber data) and 54% related to events data (which would have previously broadly aligned to traffic data).

2.18

Communication Data Items Received by Type



Legal Protection Afforded to Journalists and Lawyers

2.19
Article 8 of The European Convention on Human Rights protects the confidentiality of correspondence between individuals, and it affords enhanced protection to correspondence between lawyers and their clients. This is due to the fundamental role that lawyers play in a democratic society in defending litigants. Through a succession of decisions in Court, the area of legal privilege has been addressed including:

- Klass and Others v Germany (1978) ¬– dealt with whether there was a right to know if a person subject to surveillance had been subjected to covert powers. The Court found no violation of Article 8 observing that that powers of secret surveillance of citizens were tolerable only insofar as is necessary to safeguard the democratic institutions.

- Laurent v France (2018) – interception of written communication between a client and a lawyer, absent suspicion of an unlawful act, could not be justified and did not fulfil a pressing social need so as to be necessary within the meaning of Article 8.

- Versini-Campinchi and Crasianski v France (2016) – interception of a telephone call which disclosed a lawyer had breached the embargo on beef imports from the UK during the BSE crisis. The Court held that the transcript gives rise to the presumption the applicant lawyer had committed an offence and the domestic courts had satisfied themselves the transcript did not infringe upon her client's rights of defence. The fact that the applicant was the first applicant's lawyer did not suffice to constitute a violation of Article 8.

2.20
Similarly, Article 10 of The European Convention on Human Rights provides protections for journalistic sources. The press have been afforded a broad scope of protection in the Court's case law with regard to the confidentiality of journalistic sources. In the leading case on the issue, Goodwin v UK (1996), it is noted:

> *'Protection of journalistic sources is one of the basic conditions for press freedom. … Without such protection, sources may be deterred from assisting the press in informing the public on matters of public interest.'*

2.21
However the Court has held this is not absolute and journalists can be required to disclose their sources in certain cases, each case is fact specific:

- Nordisk Film & TV A/S v Denmark (2005)- where the Court held that requiring a journalist to disclose research material obtained by going undercover with a paedophile association for a documentary was a proportionate interference with the journalist's freedom of expression and that this was justifiable for the prevention of the serious child sexual abuse;

- Jecker v Switzerland (2020) – where the Court dealt with the requirement to testify to identify journalistic sources following the publication of a story dealing with cannabis over a protracted period of time. The Court found that the requirement to identify sources was generally framed and did not adequately address the issue of necessity or the balancing exercise required when journalistic sources were to be identified.

2.22
The Chief Constable is personally committed to upholding and ensuring the protection afforded to lawyers and journalists is provided by the officers and staff within the Police Service of Northern Ireland. The Chief Constable personally has detailed and extensive experience in the use of covert powers. Throughout his career he has carefully identified, considered, balanced and respected the rights of lawyers and their clients, and journalists and their sources, as provided for by law. He also recognises the commitment of the PSNI over the last two decades in embedding human rights in every area of practice. The Police Service of Northern Ireland has, in many aspects of policing, led the way in developing a human rights compliant approach. In many ways this is unsurprising given the programme of reform and change envisaged by and delivered as a result of the Patten Report. This is equally true of our approach to covert policing.

2.23
In the UK domestic law affords journalistic sources a number of protections including Section 10 of the Contempt of Court Act 1981, which was introduced in response to a decision of the European Court of Human Rights in 1979[6] in the case of Sunday Times v United Kingdom. Section 10 provides:

> *'No court may require a person to disclose, nor is any person guilty of contempt of court for refusing to disclose, the source of information contained in a publication for which he is responsible, unless it be established to the satisfaction of the court that disclosure is*

[6] *(1979) 2 EHRR 245 –see http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-57584#{"itemid":("001-57584")}.*

necessary in the interests of justice or national security or for the prevention of disorder or crime.'

2.24

In addition the Public Interest Disclosure (Northern Ireland) Order 1998 protects those who make qualifying disclosures in the public interest and allows a person to bring an employment law complaint for victimisation. To qualify for protection under the order, the disclosure the person makes must, in the reasonable belief of the worker making the disclosure, show or tend to show one of the following:

- that a criminal offence has been committed, is being committed or is likely to be committed,
- that a person has failed, is failing or is likely to fail to comply with any legal obligation to which he is subject,
- that a miscarriage of justice has occurred, is occurring or is likely to occur,
- that the health or safety of any individual has been, is being or is likely to be endangered,
- that the environment has been, is being or is likely to be damaged, or
- that information tending to show any matter falling within any one of the preceding sub-paragraphs has been, is being or is likely to be deliberately concealed.[7]

Most often this is referred to as *'whistleblowing'*, and within the Police Service a specific policy[8] outlines how officers and staff may make a qualifying disclosure.

2.25

For policing purposes in Northern Ireland the Police and Criminal Evidence (Northern Ireland) Order 1989 (PACE) contains similar protective provisions in respect of both journalistic material, which is deemed 'excluded material', and items subject to legal privilege. Article 11(2) of PACE provides:

'any statutory provision passed or made before the making of this Order under which a search of premises for the purposes of a criminal investigation could be authorised by the issue of a warrant to a constable shall cease to have effect so far as it relates to the authorisation of searches—

(a) for items subject to legal privilege; or
(b) for excluded material;'

Schedule 1 of PACE then mandates a procedure for access which includes:

- Notice to affected parties;
- Judicial oversight;
- Prior approval.

[7] *Section 67B (1) Public Interest Disclosure (NI) Order 1998.*
[8] *See Service Instruction SI31/17 available at Whistleblowing 16 April 2024_0.pdf (psni.police.uk)*

The Kennedy Inquiry

2.26

Not withstanding the above legal protections, in 2014 there was mounting public concern that the Metropolitan Police and Kent Police had used powers within the 2000 Act to seek to identify journalist sources for the Andrew Mitchell and Chris Huhne investigations. As a result the then Interception of Communications Commissioner, Rt Hon. Sir Paul Kennedy, exercised his powers to conduct a full inquiry into authorisations for communications data in respect of journalistic sources[9] (The Kennedy Inquiry). The reference period for the inquiry was October 2011 to October 2014. The remit of this review went beyond the activities of the Metropolitan Police Service and extended to other UK police services, encompassing a review of 34 investigations and some 608 applications for communication data.

2.27

In the resulting report to the Prime Minister in February 2015 IOCCO found that the 2000 Act and the 2007 Code did not give any guidance on how, in practice, the necessity and proportionality exercise should differ for applications for communication data which may seek or touch on journalistic material. IOCCO, however found the 2007 Code lacked clear guidance for designated Inspectors and Superintendents on how they should apply the principles of necessity, proportionality and collateral intrusion for journalists or to take account of the added dimension that the requirement may lead to the identification of journalistic sources, either intentionally or not. The Kennedy Inquiry was not mandated to consider the lawfulness of the use of the powers, but rather whether they were being used in an appropriate way. In response to the Review, a new Code of Practice was issued in March 2015.

2.28

The Police Service of Northern Ireland cooperated fully with this Inquiry. PSNI records relevant to the terms of reference for the inquiry, which overlap in part with the scope of this report, indicate there were six investigations conducted relating to suspected illicit relationships between public officials who were suspected to be the journalists' sources. All bar one of the investigations were led by the Professional Standards Department. These features mirror the findings of the Kennedy Inquiry elsewhere in the UK.

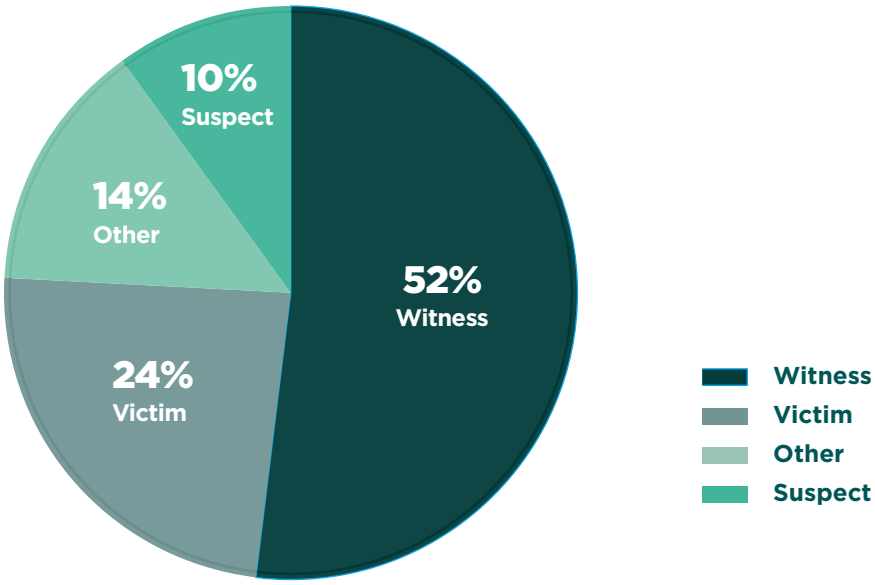
[9] *See IOCCO Inquiry into the use of Chapter 2 of Part 1 of RIPA to identify journalistic sources.*

Statistical Data – Journalistic Communication Data

2.29

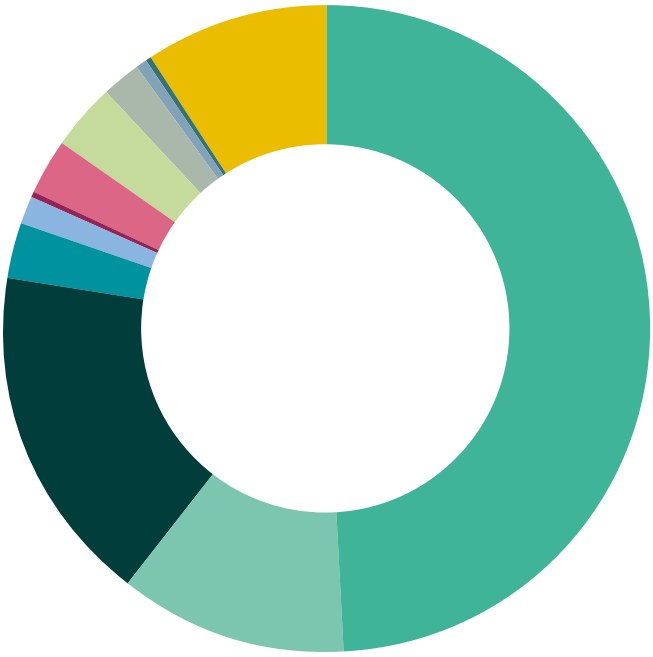
In the reporting period (1st January 2011 to 31st March 2024) there were 323 applications relating to a person who was identified as a journalist. Of those 323 applications they were categorised according to their relationship to the offence being investigated. As noted by IOCCO in their 2017 Annual report the journalist's profession is very often not relevant to the application and the data is sought solely because the person is a victim or suspect or witness to a crime. For example, a journalist who is receiving harassing comments on a social media platform or phone calls or texts is a victim of harassment. The police officer investigating that offence will seek communication data to progress the investigation and identify the person harassing the journalist, in the same way as they would for any other victim. It is a legitimate and necessary line of investigation to be pursued, without which the offence reported by the victim, who is also a journalist, could not be investigated. In that regard their profession can often be irrelevant to the application. The below chart shows the identified connection of the journalist to the offence under investigation.

Journalist Relationship to the Offence



2.30
The below chart shows the nature of the investigations for which communications data was sought.

Journalist Authorisations by Investigation Type



Terrorism	49.23%
Misconduct in Public Office	11.46%
Harassment	17%
Sexual offences	2.79%
Breach of Court Order	1.24%
Breach of DPA	0.31%
Telecoms Offences	2.79%
Murder	3.41%
Fraud	1.86%
Protection of Life	0.62%
Threats to Kill & associated offence	8.98%
Theft and related offences	0.31%

Of all applications, 76.8% were authorised to obtain communication data, the remaining 23.2% were variously rejected by the Office of Communications Data Authorising Officers or the Police Service of Northern Ireland's single point of contact (12.6%)[10] , or simply not proceeded with by the applicant (10.5%).

[10] *Rejected applications are not currently broken down between OCDA and the PSNI single point of contact therefore a consolidated figure for all rejected applications is provided.*

Journalistic Sources

2.31
To assist with meaningful insights as to when the journalist's profession is **relevant** to the communication data being sought, it should be considered whether the authorisation seeks to identify a journalistic source. Applying that test, a much smaller number of applications within the reporting period were authorised; 10 applications were made across four investigations. The primary nature of the investigations related to the unauthorised disclosure of Police Service of Northern Ireland information or documents.

2.32
All of the investigations where communication data was sought were connected to, in some way or another, a crime. However they would not have objectively been assessed as having met the 'serious crime' threshold that would later (post-2015) become a requirement of such applications, firstly codified in the 2015 Code of Practice, then later legislated for in the 2016 Act. This is entirely consistent with the findings of the Kennedy Inquiry from their examination of UK policing practice at that time.

2.33
Data Protection and Misconduct in Public Office were a frequent feature of authorisations for communication data concerning journalists, replicating the pattern identified in the Kennedy Inquiry of 2015. Where a public official improperly discloses information they most often will be properly investigated for 'data protection' and 'misconduct in public office' offences. Current IPCO inspections continue to examine this area.

2.34
The below chart shows the breakdown of authorisations by designated Inspectors and Superintendents within the Police Service of Northern Ireland in the reporting period, before judicial approval was introduced as a requirement in 2015.

Types of Communication Data Obtained

Types of Data Sought:

- **Subscriber**
- **Traffic**

2.35
Although Superintendents were required to authorise only applications for traffic data, with Inspectors able to authorise subscriber details, the practice in the Police Service of Northern Ireland was that designated Superintendents authorised all of these applications.

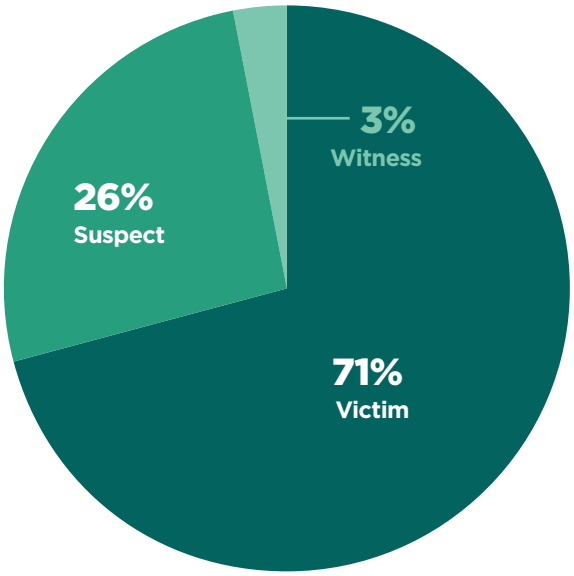
2.36
Overwhelmingly the investigations were commenced as a result of press coverage which involved the unauthorised disclosure of information that might potentially compromise ongoing operations or activity. It is clear that had the threshold then been that now defined as 'serious crime', the number of authorisations for communication data in relation to journalists would have been substantially reduced.

Statistical Data –Lawyers' Communication Data

2.37
In the reporting period (1st January 2011 to 31st March 2024) there were 500 applications relating to a person who was identified as a lawyer. Detailed data for applications during the period 1st January 2011-21st August 2017 is not currently available, therefore only data for the period from 21st August 2017 to 2024 is provided below. Where possible the applications were categorised according to their relationship to the offence being investigated. As noted above, very often the profession is not relevant to the application for communication data but the communications data is sought solely because the person is a victim or suspect or witness to a crime. In that regard their profession can often be irrelevant to the application. The below chart shows the identified connection of the lawyer to the offence under investigation. As shown below, in over 70% of investigations the lawyer was the victim of the crime under investigation.

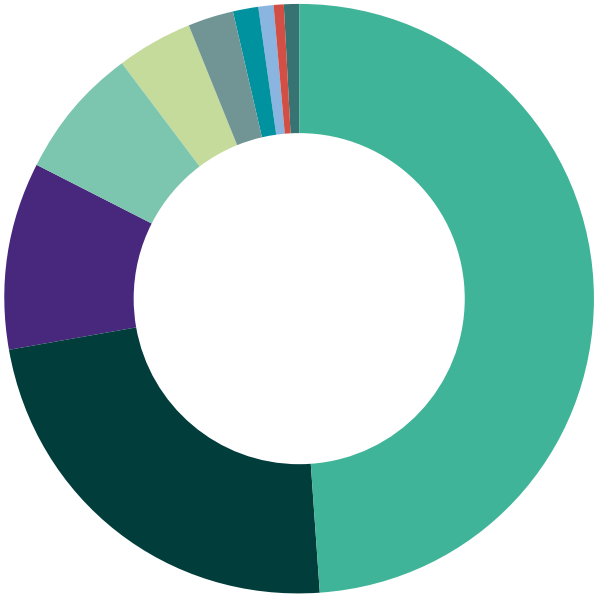
Lawyer Relationship to the Offence

Aug 2017 - Present



2.38
The below chart shows the nature of the investigations for which communications data was sought.

Lawyer Authorisations by Investigation Type



Terrorism	35.40%
Murder	9.73%
Child Sexual Exploitation	3.54%
Fraud	5.31%
Harassment	28.32%
Threats to Kill	13.27%
Threats to Commit Arson	0.88%
Self Harm Concerns	1.77%
Threats to commit GBH	0.88%
Theft Offences	0.88%

2.39
Of all applications, 73% were authorised to obtain communication data. The remaining 27% were variously rejected by the Office of Communications Data Authorising Officers or the Police Service of Northern Ireland's single point of contact (24%)[11], or simply not proceeded with by the applicant (3%).

2.40
Unlike when considering journalistic material, there are no equivalent recording systems in place to comprehensively identify and record authorisations when the lawyers' profression was relevant to the authorisation for communication data, beyond those where the authorisation itself involved a lawyer.

[11] Rejected applications are not currently broken down between OCDA and the PSNI single point of contact therefore a consolidated figure for all rejected applications is provided.

This is because, as described at paragraph 2.16, communication data relates to the who, where and when of a communication but not what was said. Legal professional privilege, that essential element critical to maintaining the confidentiality between lawyers and clients, relates primarily (but not exclusively) to what was said between them. It is more relevant when considering the powers in paragraph 4.3-4.7.

Lawful Business Monitoring

2.41

As a regulated profession, subject to clear standards set out in the Code of Ethics and Staff Handbook, the Police Service of Northern Ireland uses lawful business monitoring to ensure our police officers, our police staff and our contractors are behaving lawfully and in line with our standards and values and in a way which the public would expect. Lawful business monitoring is also used to improve how we respond to incidents, learn from our mistakes and to improve the service we deliver to the public. Reported commentary on aspects of lawful business monitoring have misrepresented this practice in the Police Service of Northern Ireland, describing it as a 'defensive operation' targeting journalists. More details on this can be found in Appendix A.

2.42

Lawful business monitoring is authorised under the Investigatory Powers (Interception by Businesses etc. for Monitoring and Record Keeping purposes) Regulations 2018[12] . Recent research from the Information Commissioner's Office suggests nearly one in five people believe this type of monitoring is conducted in their workplace. It is routinely disclosed in criminal and disciplinary proceedings for our officers and staff. It is not a covert tactic, indeed all officers and staff are informed of the operation of lawful business monitoring on PSNI systems. Monitoring can include:

- Monitoring work emails, files, calls or messages;
- Monitoring timekeeping, access or clocking in/out;
- Monitoring internet activity or keystrokes;
- Taking screenshots or webcam footage;
- Using monitoring software or productivity tools;
- Recording audio or video;
- Tracking location whilst working;
- Reviewing use of social media channels.

[12] *Formerly the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000*

2.43
Examples of business monitoring include where the Police Service seeks to identify if a police officer has contact with a vulnerable person they have met in the course of their duty, or if a police staff member uses inappropriate language when speaking to a member of the public on the phone, or to identify if an officer is in contact with a person involved in the supply of drugs. These are all issues of concern for the Police Service in ensuring the highest standards in our officers and staff, as the public would rightly expect. The Police Service has a number of policies which provides clear direction for officers and staff in this area:

- **Off Duty Standards** – which deals with the issue of inappropriate associations for a member of the PSNI. It defines those as those which have the potential to, or are likely to:
  - Compromise the member of staff (such as associating with known criminals);
  - Compromise the operations or activity of the Police Service; and or
  - Compromise the reputation of the Police Service.

- **Maintaining Professional Boundaries** – which deals with interactions with members of the public where the officer or staff member has had a professional interaction with them, as well as inappropriate relationships within the Police Service of Northern Ireland.

- **Acceptable Use Standard** – which deals with the acceptable use of all information and communication technology provided by the Police Service, how monitoring will be conducted and sets clear expectations that there will be no privacy when using PSNI supplied information or communication technology.

2.44
This process is normally managed by the Anti-Corruption Unit who seek to identify police officer and police staff misconduct or criminal offences. It was reviewed in the 2023 His Majesty's Inspectorate of Constabulary, Fire and Rescue Services (HMICFRS) report on police effectiveness, efficiency, vetting and standards in the Police Service of Northern Ireland noting:

> *'This includes auditing force systems and social media accounts.*
>
> *We were told the service couldn't monitor some mobile devices issued to personnel. This makes it more difficult to keep information safe and is a potential security and corruption risk. The service should make sure it can monitor effectively all work-issued mobile devices.'*

Indeed HMICFRS found there was a need for increased lawful business monitoring to ensure police issued mobile phones were not being misused for corrupt purposes.

2.45
In practice this means the Professional Standards Department (PSD) conduct IT audits and monitor the use by police officers, police staff and contractors of police service supplied systems. Where there is reason to suspect that a particular officer has been misusing those systems there may be an audit of the systems to ensure that officer has complied with service policy. However where the identity of the suspected officer remains unknown a different investigatory approach will be required. The approach adopted depends on the nature of information available as shown below:

Example 1:
PSD receive information that Police **Officer 1234** has been inappropriately passing information to **Mr A**, a person convicted of drugs supply. An audit of Police Officer 1234's system access and use will be conducted.

Example 2:
PSD receive information that **Mr A**, a person convicted of drugs supply, has been receiving information from an unknown police officer. An audit of all PSNI systems will be conducted to identify any employee who has viewed Mr A's records or been in contact with him recently to identify the unknown officer.

2.46
An investigative method previously used in lawful business monitoring within the Police Service was to audit systems, including police telephone systems, to identify serving officers who had been in contact with known subjects of interest in particular investigations. Subjects of interest were identified through PSD investigations and kept under review during the course of the investigation. Those subjects of interest were identified from a range of PSD investigations including:

- Related to the unauthorised disclosure and theft of police information;
- Corrupt payments to public officials;
- Police officers paying for sexual services;
- Police officers having inappropriate contact with victims and witness.

2.47
This method was reviewed in March 2023 and has been discontinued, as its effectiveness was limited. There are current no plans to use the tactic within the Police Service of Northern Ireland, however it may be used in the future. Public commentary on the use of this tactic has focused on its use for investigations related to the disclosure of police information, particularly where that information may be disclosed to journalists. The case of R v Chapman & Ors[13] grappled with the balance to be struck when considering the offence of misconduct in public office,

[13] *(2015) EWCA Crim 539 available at R -v- Chapman & Ors; R -v- Sabey (judiciary.uk)*

particularly considering officials such as police officers, prison officers etc. at para 33:

> *'...In a democratic society the media carry out an important role in making information available to the public when it is in the public interest to do so, not simply (as the judge pointed out) because the public may be interested in it.* ***Those employed by the state in public office will generally be in breach of the duty owed by them to their employers or commanding officers by providing unauthorised information to the press. However, information is sometimes provided by such persons in breach of that duty where the provider of that information may benefit the public interest rather than harm it. The provision of the information may well in such a case be an abuse of trust by the office holder to his employer or commanding officer, even if the disclosure of the information may be in the public interest. It may therefore result in disciplinary action and dismissal of the officer holder.*** *That is because the abuse of the trust reposed in the office holder by the employer/commanding officer in such a case is viewed through the prism of the relationship between the office holder and his employer or commanding officer.* ***That is not the prism through which a jury should approach the issue of the abuse of the public's trust in an office holder.***
>
> ***34. The offence requires, as the third element, that the misconduct must be so serious as to amount to an abuse of the public's trust in the office holder' (emphasis added).***

2.48

The Court reinforced that the offence of misconduct in public office requires a high threshold of misconduct. The misconduct must be so serious so as to amount to an abuse of the public's trust in the office holder. Even in cases where the disclosure of the information may benefit the public interest so as to not amount to a criminal offence, the public official may be liable to disciplinary action and dismissal for the disclosure and a fundamental breach of trust. None of this affects the protection afforded to the journalist who receives the disclosed information within domestic UK law and the European Convention on Human Rights. The Court recognised the tension that exists between journalists seeking to protect their sources and public bodies obliged to investigate unlawful disclosures made by their employees or contractors.

March 2015 - Present

2.49
The revised Code was issued to take account of the issues identified in the Kennedy Inquiry in March 2015 and dealt with the particular issues relating to journalists and lawyers at section 3.72-84. The additional requirements provide for judicial oversight in some circumstances and in summary the revised Code requires:

- Clear recording requirements in respect of all applications concerning members of those in sensitive professions;
- Requirements that applications seeking to identify journalistic sources must be made to a Judge via a Police and Criminal Evidence (NI) Order 1989, production order (until new legislation introduced judicial oversight);
- Central recording requirements for applications relating to journalistic material including the relevant considerations.

2.50
Whilst the term 'sensitive profession' is not used in the Code, a partial definition is provided at 3.73 as 'member of a profession that handles privileged or otherwise confidential information, including medical doctors, lawyers, journalists, Members of Parliament or ministers of religion'. Accordingly from 2015 onwards the term 'sensitive profession' became part of the reporting and recording terms within the 2000 Act. However there are limitations to 'sensitive professions', including how non-governmental organisations, and those who work for them are identified and afforded appropriate protection within the overall regime. This is an area that the Chief Constable is particularly alert to and has asked that it be explored more fully in the plan detailed in paragraph 5.8.

2.51
For the period from March 2015 to 2019 applications for communications data to identify a journalistic source were required to follow the PACE Special Procedure process. This was because, following the Kennedy Inquiry, there was a requirement for judicial oversight, however this required new legislation, and that was not available until 2019. The process followed between March 2015 and 2019 is described briefly at paragraph 2.25 above. However it is detailed in Schedule 1 of the Police and Criminal Evidence (NI) Order 1989, where it provides a number of safeguards including:

- Notice to affected parties;
- Judicial oversight;
- Prior approval.

Production Orders granted in accordance with Schedule 1 are not detailed further here for the period 2015-19 as the power was not covert; application was made on notice to parties, and the power was not a power within either the 2000 or 2016 Act.

2.52
Judicial oversight was ultimately introduced by the Investigatory Powers Act 2016 and commenced in February 2019 for this purpose. Section 61 introduced additional legal thresholds for the granting of authorisations for communications data, namely:

- The data must be necessary for a specific investigation or operation; and

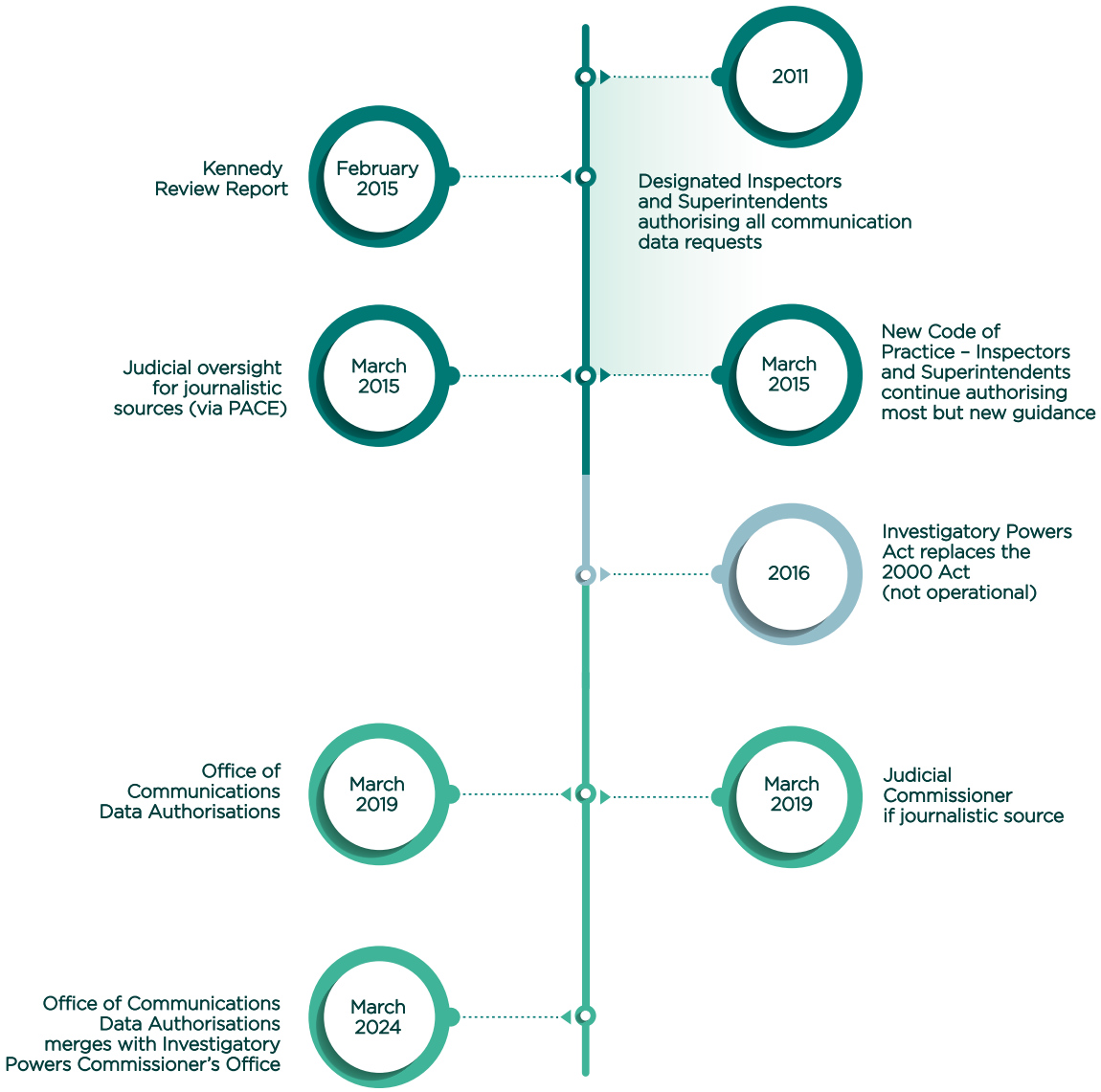
- The authorised conduct is proportionate to what is being sought to be achieved; and

- Authorisations are considered independently by the Office of the Communications Data Authority (ODCA) (replacing designated Superintendents and Inspectors within the PSNI); and

- Where the authorisation relates to a journalistic source approval from a Judicial Commissioner is required

2.53

The effect of these changes can be seen in the timeline below.



3: Conduct Powers

3.1
Conduct powers are primarily used to regulate the conduct of police officers in using covert policing tactics. Covert tactics are those tactics which are carried out in such a way that the intended person subject to them is unaware that those tactics are, or may be, being used. Due to the covert nature of these tactics they are highly sensitive and strictly regulated. The main powers are detailed below along with total numbers of authorisations relating to journalists or lawyers in the reporting period. Given the sensitivity of the powers and so as not to enable the identification of individuals, it is not possible to provide further statistical information on the use of these powers beyond aggregated data for the reporting period. As the powers get more intrusive, the authorisation required similarly increases, until for example the authority of the Secretary of State, on application of the Chief Constable is required. Neither the Chief Constable Jon Boutcher, nor his Deputy Chris Todd, as senior authorising officer, have considered any applications seeking authorisation for conduct powers in respect of journalists or lawyers since they were appointed in October 2023.

Covert Human Intelligence Source

3.2
A Covert Human Intelligence Source (CHIS) is an informant or an undercover officer. They support the functions of certain public authorities by providing intelligence covertly. A CHIS under the age of 18 is referred to as a Juvenile CHIS. CHIS are authorised in accordance with Part II of the 2000 Act.

3.3
Another type of CHIS is known as a "relevant source". This is the term used to describe staff from a designated law enforcement agency that are trained to act as undercover operatives and are subject to an enhanced authorisation and oversight regime.

3.4
A CHIS may be authorised to participate in criminal conduct in specific circumstances, namely in the interests of national security; for the purpose of preventing or detecting crime or of preventing disorder; or in the interests of the economic well-being of the United Kingdom[14].

3.5
In the reporting period there were four CHIS authorised in respect of journalists or lawyers.

[14] *See Covert Human Intelligence Sources (Criminal Conduct) Act 2021*

Directed Surveillance

3.6
This is surveillance that is covert but is not carried out in a private residence or vehicle. It can include covert recording of a person's movement's, conversations and other activities. Directed surveillance is authorised in accordance with Part II of the 2000 Act by an Authorising Officer of Superintending rank.

3.7
Authorisations for directed surveillance require a number of essential elements:

1. The surveillance must be covert, but not intrusive; and

2. It must be conducted for the purposes of a specific investigation or operation; and

3. It must be likely to result in the obtaining of private information about a person (whether or not that person is specifically known or identified); and

4. It is conducted otherwise than by way of an immediate response to circumstances or events the nature of which make it not reasonably practicable to seek an authorisation under Part II of the 2000 Act.

Private information includes any information relating to a person's private or family life. As a result, private information is capable of including any aspect of a person's private or personal relationship with others, such as family and professional or business relationships.

3.8
In the reporting period there was no authorised use of this power in respect of journalists or lawyers.

Intrusive Surveillance

3.9
This is similar to directed surveillance but it is conducted in a private residence or vehicle. This surveillance may be carried out using an eavesdropping device in residential premises or in private vehicles. It may also involve the covert presence of a listening device to capture conversations and ensure that the person subject to the surveillance is unaware that surveillance is taking place. Intrusive surveillance is authorised in accordance with Part II of the 2000 Act by a Senior Authorising Officer, in the Police Service of Northern Ireland this is the Chief Constable or Deputy Chief Constable.

3.10
In the reporting period there was no authorised use of this power in respect of journalists or lawyers.

Property Interference

3.11
This power is often used in conjunction with intrusive surveillance authorisations. Property interference provides lawful authority for the covert physical interference with physical property, and wireless telegraphy. This power is often used in conjunction with intrusive surveillance to authorise, for example, police to trespass to covertly install a listening device on another's property. Property Interference is authorised in accordance with section 93 of the Police Act 1993 by the Chief Constable or Deputy Chief Constable.

3.12
In the reporting period there was no authorised use of this power in respect of journalists or lawyers.

4: Content Powers

4.1
Content powers are highly intrusive covert powers which are now provided by the 2016 Act. There are two primary content powers available to the Police Service of Northern Ireland, however neither can be exercised alone. Content powers provide a lawful basis to:

- Obtain content of communications in transmission in accordance with Part 2 of 2016 Act. This power is known as targeted interception.

- Interfere with electronic equipment so as to obtain information or communication in accordance with Part 5 of 2016 Act. This power is known as targeted equipment interference.

4.2
For both powers the Police Service of Northern Ireland is required to apply in advance for a warrant prior to authorisation of the activity of interception or interference.

Targeted Interception

4.3
In the case of targeted interception the approval of a Secretary of State, or in their absence a Minister of State for Northern Ireland is required. The grounds on which the Secretary of State may issue a warrant are contained within section 20 of the 2016 Act, they are that the warrant is necessary:

(a) in the interests of national security,

(b) for the purpose of preventing or detecting serious crime, or

(c) in the interests of the economic well-being of the United Kingdom so far as those interests are also relevant to the interests of national security (but see subsection (4)).

4.4
As outlined at paragraph 1.6 the Chief Constable, Deputy Chief Constable and every police officer are prohibited by section 57 of the 2016 Act from detailing any use of this tactic. Reference can only therefore be made to data already published by IPCO using an annual dataset for the UK as a whole. Each year IPCO request feedback on the value of the statistics published and the transparency the statistics provide to the public and stakeholders.

4.5
The IPCO 2022 Annual report showed there were 4574 authorisations for the whole of the UK and for all warrant granting departments, i.e. not restricted to UK police services.

4.6
Until 2020 data was not consistently recorded on the number of instances involving sensitive professions, including lawyers and journalists. However there are strict provisions in place within the Codes of Practice governing the use of this power and this is a key area of focus for IPCO in their annual inspection. Annual data aggregated from across the UK, compiled by IPCO, shows that confidential material, including material belonging to lawyers, journalists and other sensitive professions, was only sought to be obtained in a small number of warrants as shown below.

	Total TI (All UK)	LPP Sought	LPP Possible	Sensitive Professions
2020	3649	12	359	35
2021	3634	11	187	11
2022	4574	29	211	20

Targeted Equipment Interference

4.7
Similarly Targeted Equipment Interference, which is a relatively new power (only introduced in 2018) is subject to certain prohibitions on disclosure. Accordingly only published IPCO aggregated statistics, from across the UK, is outlined below. The power is currently authorised on average 1,100 occasions each year across the UK. Annual data from IPCO would show that confidential material, which would include material belonging to lawyers and journalists, was only sought or likely to be obtained in a small number of warrants.

	Total TEI (All UK)	LPP Sought	LPP Possible	Sensitive Professions
2020	2957	14	207	66
2021	3175	15	64	14
2022	5327	29	499	63

5: Accountability Arrangements

5.1
Part 8 of 2016 Act provides for oversight arrangements for the covert powers outlined above, which provides for:

- Investigatory Powers Commissioner's Office; and

- Investigatory Powers Tribunal;

In addition the Chief Constable recognises and acknowledges the exercise of these powers is a matter of significant interest to the Northern Ireland Policing Board, and that he is fully accountable to the Policing Board for all policing operations as explicitly set out in the St Andrews Agreement. The Chief Constable is personally and professionally committed to ensuring and reassuring the Policing Board that the covert powers available to him are authorised and used in a way which is proportionate, lawful and necessary.

Investigatory Powers Commissioner's Office

5.2
Part 8, Chapter 1 of the 2016 Act provides for an Investigatory Powers Commissioner Office (IPCO), supported by a number of Judicial Commissioners, to be appointed by the Prime Minister, on joint recommendation from the Lord Chancellor, the Lord Chief Justice of England and Wales, the Lord President of the Court of Session and the Lord Chief Justice of Northern Ireland. To be eligible to be appointed the Commissioners must have held high judicial office and are appointed for a term of three years. IPCO are required to keep under review, including by way of audit, inspection and investigation the exercise of powers by public authorities relating to:

- Interception of communications;

- Acquisition or retention of communications data;

- Acquisition of secondary data or related systems data;

- Equipment interference.

5.3
In practice IPCO discharge these functions through a series of inspections and audits of the powers on an annual and thematic basis, identifying trends, issues of concern and learning. During their oversight activity they are afforded unrestricted access to the underlying authorisations and material to assess compliance with the requirements of the legislation and the relevant codes of practice, in accordance with section 235 of IPA. The current Investigatory Powers Commissioner is the Right Honourable Sir Brian Leveson, a former Lord Justice of Appeal, and Chairman of the Sentencing Council. He is supported by 15 Judicial Commissioners, including Sir Declan Morgan, former Lord Chief Justice of Northern Ireland. Each year IPCO publish an

annual report which outlines the findings of their inspection activity, the nature and extent to which the powers have been used and any areas of concern the Commissioner identifies in accordance with section 234. This report is provided to the Prime Minister, published and laid before Parliament. Previous reports are available by **ipco.org.uk/publications/annual-reports/.**

5.4
The Police Service of Northern Ireland was last inspected by IPCO from 29th April to 3rd May 2024. The inspection was led by Sir Declan Morgan. IPCO identified no issues of non-compliance during their inspection with regards to the management of confidential information in compliance with the relevant Codes of Practice. These inspections continue to have a focus on journalistic material, legal privilege and other confidential material relating to sensitive professions. The last Communication Data inspection was from 12th – 14th March 2024 and also involved Sir Declan Morgan, overall it found PSNI acted lawfully in acquiring communication data for a correct statutory purpose, with IPCO commending officers and staff for their diligence and effort. The Chief Constable and Deputy Chief Constable are personally debriefed on the findings of the inspections and at the most recent inspection the Chief Constable sought specific assurance from IPCO on the issue of authorisations related to journalists, lawyers or sensitive professions and whether any issues of concern were identified during their inspection activity and was advised that there were no issues identified.

5.5
The Police Service of Northern Ireland has fully engaged with and will continue to cooperate fully with IPCO. Additionally in 2023 and 2024 the Policing Board's Human Rights Advisor has been directly engaged in IPCO Inspections and was present during the debriefs with the Chief Constable and Deputy Chief Constable.

Investigatory Powers Tribunal

5.6
The Investigatory Powers Tribunal (IPT) was established under Part IV of the 2000 Act. The purpose of the IPT is to consider human rights complaints in relation to the exercise of covert powers contained within primarily IPA, RIPA and a number or ancillary pieces of legislation. It is an independent Court which considers two types of complaints:

- Human rights complaints;
- Unlawful interference complaints.

5.7
The Tribunal does not ordinarily hold hearings on complaints submitted, but considers papers submitted by the complainant. The Tribunal may then hold a hearing where there are difficult issues of fact or law to be determined. When first established the Tribunal only sat in private, however since 2003 the Tribunal has adopted a position that it should sit in public, where possible.

5.8
The Police Service of Northern Ireland has fully engaged with and will continue to cooperate fully with the IPT. However we are unable to comment where individuals speculate on whether they have been subject to the use of covert powers or not. The IPT remains the appropriate body to consider complaints in relation to the use of covert powers and the Chief Constable would encourage anyone with concerns to engage with the Tribunal directly. Full details on how to make a complaint can be found on their website, including details on how to download the relevant forms, or at **investigatorypowerstribunal.org.uk/how-to-make-a-complaint/.**

Chief Constable's Assurance Plan

5.9
To further reassure the public and the Northern Ireland Policing Board that the covert powers available to the Police Service have been and continue to be used in a way which is lawful, proportionate and necessary, the Chief Constable has appointed Angus McCullough KC, of 1 Crown Office Row, as a special reviewer to investigate the concerns expressed publicly by a number of stakeholders and provide an independent assessment to ascertain and confirm the position.

5.10
These concerns relate to possible covert surveillance of individuals or groups that have a special status within democratic societies. The terms of reference for the scope of Mr McCullough KC's role will be endorsed by the Chief Constable following agreement between him and a steering group consisting of the following proposed stakeholders and experts;

- Baroness Nuala O'Loan
- Martha Spurrier BL
- Amnesty International UK
- Committee on the Administration of Justice
- Alyson Kilpatrick BL, Chief Commissioner of the Northern Ireland Human Rights Commission
- David A Lavery CB, Chief Executive of the Law Society of Northern Ireland
- Seamus Dooley, Assistant General Secretary of the National Union of Journalists

5.11
Angus McCullough KC is recognised as a leading Special Advocate in practice in the United Kingdom. In that capacity he has unparalleled experience of probing, challenging, and assessing closed material. This includes evaluating such material with a view to contending for it to be disclosed beyond the scope of closed proceedings, if necessary by gisting or making such redaction as is strictly necessary in order to protect any legitimate public interest. It is envisaged that he will be given entirely unrestricted access to Police Service of Northern Ireland records, material, and personnel for the purposes of his reviewing function. However his role would not extend to anything that is currently within the scope of any pending judicial or IPT proceedings. It is proposed that he would engage closely with the steering group in performing his role.

5.12
At the conclusion of his work Mr McCullough KC will provide the Chief Constable with a report setting out his findings in relation to the application, authorisation, conduct and use of surveillance powers by the Police Service of Northern Ireland during the period from 1st January 2011 – 31st March 2024, in relation to journalists, lawyers, non-governmental organisations and all other sensitive professions or other identified groups (as agreed by the Chief Constable and Mr McCullough KC). He is also to be asked to make any recommendations as he sees fit in relation to practice and procedures in relation to the matters within the scope of his review.

5.13
Mr McCullough KC will be available to address the Northern Ireland Policing Board as and when required about the review.

5.14
The Chief Constable will publish the final report received from Mr McCullough KC.

6: Conclusion

6.1
The Chief Constable has sought to be as open and transparent as is possible, in the provision of information available to him, through this report. This report is intended to inform and reassure the public and the Northern Ireland Policing Board that all covert and surveillance powers available to the service are being used in a way that is lawful, proportionate, and necessary. The information and records available to the Chief Constable demonstrate that there was not a widespread practice of surveilling journalists or lawyers within Northern Ireland. Rather, the use of covert powers in respect of journalists and lawyers was overwhelmingly in support of an investigation into a crime where their occupation was not a relevant factor. Most often they were victims or witnesses to crimes unrelated to their profession. Overall the number of authorisations for communications data for journalists accounted for less than 0.5% of the total authorisations granted since 2011.

6.2
In the small number of cases where authorisations were granted to identify journalistic sources, the Police Service sought to apply the Code of Practice available in law at the relevant time. However, it is acknowledged now that the Code did not provide adequate safeguards when considering authorisations to identify a journalistic source prior to 2015. This was not an issue unique to the PSNI, and indeed applied throughout the UK, until the introduction of a new Code in March 2015, and then new legislation in February 2019.

6.3
Since March 2015 all applications to identify a journalist's source required the approval of a judge in some form or another, either through PACE or by a Judicial Commissioner. This provides robust, independent scrutiny and acts as an effective safeguard to the powers available to police in this area. Whilst the Chief Constable has a wide range of surveillance and covert powers available to progress investigations, they have not, in the main, been directed towards journalists or lawyers in the reporting period, since 1st January 2011.

6.4
More widely there are robust, regular and probing inspection arrangements with IPCO to ensure all the powers available to the Chief Constable are used lawfully and appropriately now. They specifically consider the areas of journalistic and legally privileged material in every inspection and the Chief Constable has sought specific assurance on this. Nevertheless, recognising the need to provide wider reassurance to the public, the Chief Constable has commissioned an eminent independent counsel, Mr Angus McCullough KC, to conduct a further review. This demonstrates his deep and on-going commitment to the appropriate and proportionate use of these powers in accordance with the law.

Appendix A :

Statement from Chief Constable Jon Boutcher regarding commentary on Investigatory Powers Tribunal and announcement of the McCullough Review 3rd June

Chief Constable Jon Boutcher said: "Recently there has been extensive inaccurate reporting relating to documents disclosed in proceedings in an Investigatory Powers Tribunal (IPT).

"Normally, I would make no comment regarding ongoing tribunal proceedings however, in this instance, the inaccurate interpretation of the documents has given rise to serious public concern about the use or abuse of police powers. The reporting is continuing, and it is unsustainable for me as Chief Constable of the Police Service of Northern Ireland (PSNI) to make no comment. I want to put the record straight and correct the inaccurate assessment of these documents.

"The public concern arises from the misinterpretation of documents made available in redacted form at the Tribunal, at least one of which was subsequently published.

"One document refers to what is described as a 'defensive operation' conducted by the PSNI. Media outlets and commentators have interpreted this term to mean that the routine and covert surveillance of journalists in Northern Ireland took place and in particular, the monitoring of their phones. This interpretation is wrong.

"The term 'defensive operation' was the description given at a meeting by a PSNI Professional Standards Anti-Corruption officer to describe a routine Professional Standards practice.

"One of the tasks of PSNI's Professional Standards Department Anti-Corruption Unit (PSD) is to detect and deter any illicit or illegal communications by police officers and staff. Corruption in any form is a hugely serious matter. Leaking information to the media can endanger police operations and put lives at risk.

"One method of identifying and deterring illegal contact with journalists is for PSD to carry out periodic checks on phone calls made from police telephone extensions and police-issued mobile phones. The numbers called are checked against the numbers held by PSNI for journalists. There is nothing covert about this procedure. The journalists' numbers are either ones that are publicly available or are ones that the journalists have themselves supplied to PSNI as contact numbers. If an unexplained call is discovered, PSD send an email to the user of the PSNI extension, asking for an explanation.

"To further reassure people, this practice is absolutely not about identifying whistle-blowers, for which there are very clear legal protections for those who are motivated to make public interest disclosures. However, if a police officer or staff member is involved in serious criminality,

we have a duty to the public to investigate this.

"The document that refers to a 'defensive operation' also contains a list of eight redacted names. Members of the media have speculated, incorrectly, that those are the names of journalists being targeted through surveillance. In fact, the names relate to a completely different matter. The names are not those of journalists. For obvious reasons of privacy, and to protect police operations, those names have not been made public.

"There has also been speculation from further disclosure of IPT material that the PSNI similarly targeted lawyers through unlawful surveillance. The speculation arises from the disclosure of two pages of notes handwritten by an officer from Durham Constabulary. The notes cover a variety of topics. The officer wrote down two initials, followed by an indecipherable word that begins with the letters 'ph'. On the following page (with several other notes in between), he wrote the words, 'legal, proportionate and necessary'. From these pieces of information, journalists appear to have concluded that the monitoring of the telephone of a journalist's legal representative was considered to be lawful.

"The notes themselves do not give any suggestion that surveillance of a lawyer's phone was being considered. We have checked with the officer who wrote the notes who has confirmed that the interpretation is entirely wrong and no such activity occurred or was considered.

"I have decided to issue this statement to provide clarity regarding these disclosures. The documents described have been made available in unredacted form to the IPT, which will consider them fully at its hearing in October. I ask that this process be respected.

"In addition to providing this clarity on documents issued through the IPT, a report on the PSNI use of covert investigative powers in relation to journalists and lawyers (outside of the issues being examined by the IPT) has now been shared with the Northern Ireland Policing Board.

"The report has been written in such a way as to enable its release for publication, to provide further reassurance to the public about the PSNI use of surveillance powers. I do not intend to make any further comment on the ongoing IPT proceedings or the contents of the report issued to the Board."

Chief Constable Boutcher concluded: "To add further reassurance, and in line with my statutory duties to report to the Board, I have also appointed Angus McCullough KC to conduct an independent review of any PSNI use of surveillance against

journalists, lawyers and Non-Governmental Organisations or any groups that have special status. His role will not extend to anything that is currently within the scope of the IPT proceedings.

"The terms of reference of the 'McCullough Review' will be published. To provide public confidence in this review a group of respected experts and stakeholders will be consulted about these terms of reference to ensure the commissioning of the review – and thereafter its work - properly examines any additional relevant matters of concern. The group and its members are not accountable for this independent review; that sits entirely with me as Chief Constable; their role is to advise and provide direction to the work of the reviewer.

It is intended that the Group of Experts and Stakeholders will consist of:

1. Baroness Nuala O'Loan
2. Martha Spurrier BL
3. Patrick Corrigan, Northern Ireland Programme Director at Amnesty International UK
4. Daniel Holder, Director of Committee on the Administration of Justice
5. Alyson Kilpatrick BL, Chief Commissioner of the Northern Ireland Human Rights Commission
6. David A Lavery CB, Chief Executive of the Law Society of Northern Ireland
7. Seamus Dooley, Assistant General Secretary of the National Union of Journalists

"Angus McCullough KC is recognised as a leading Special Advocate in practice in the United Kingdom. It is proposed that he would engage closely with the reference group in performing his role.

"Mr McCullough KC will provide a public-facing report of his findings when the review is finished and during this work he will be available to the Northern Ireland Policing Board to report on the progress of the review."

psni.police.uk

Created by Police Service of Northern Ireland Strategic Communications and Engagement Department SCE0458/24