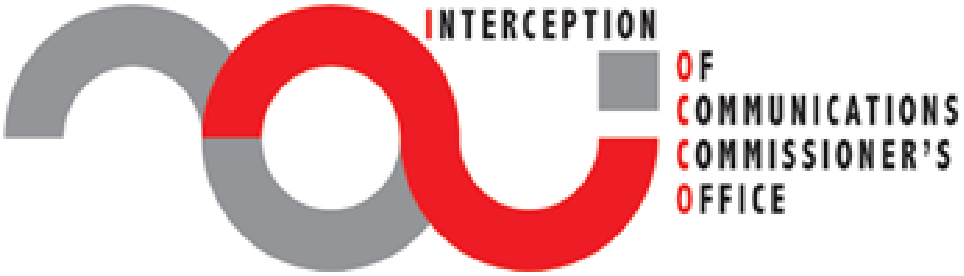


IOCCO inquiry into the use of Chapter 2 of Part 1 of the Regulation of Investigatory Powers Act (RIPA) to identify journalistic sources

Report issued 4th February 2015

Contents

Section 7

Section 8

Annexes

1 The Role of the Interception of Communications Commissioner

1.1 The Interception of Communications Commissioner ("the Commissioner") is appointed by the Prime Minister under section 57(1) of the Regulation of Investigatory Powers Act 2000 ("the Act") to keep under review, amongst other things, the acquisition and disclosure of communications data under Chapter 2 of Part 1 of the Act. The Commissioner is required to make half-yearly reports to the Prime Minister with respect to the carrying out of his functions.

1.2 The Commissioner may also, at any time, make any such *other report* to the Prime Minister on any matter relating to the carrying out of the Commissioner's functions as the Commissioner thinks fit. Due to the serious nature of the concerns reported in the media about the protection of journalistic sources, and the allegations that the police had misused their powers under the Act to acquire communications data, the Commissioner considered it necessary to undertake this inquiry and make an additional report to the Prime Minister.

2 The Purpose of the Inquiry

2.1 The purpose of this inquiry was to identify the extent to which police forces have used their powers under Chapter 2 of Part 1 of the Act to identify journalistic sources, to examine the appropriateness of the use of these powers, and to contribute to any future amendments to the legislation.

2.2 The inquiry concludes with the submission of this report to the Prime Minster and, with his approval, subsequent publication by IOCCO to the public.

3 Background to the Inquiry

3.1 On the 8th April 2014 the European Court of Justice published its ruling[1] making invalid the Data Retention Directive 2006/24/EC. The ruling identified, amongst other things, the lack of any exception for communications that are subject to an obligation of professional secrecy.

3.2 In July 2014 the UK Government Note on the European Court of Justice Judgment[2] identified that the Government would amend the code of practice for the acquisition and disclosure of communications data ("the Code") ensuring that where there may be concerns relating to professions that handle privileged material additional consideration would be given to the level of intrusion.

3.3 During September and October 2014 and more recently the press published their concerns that communications data relating to journalists had been acquired as part of the Metropolitan Police Service's (MPS's) Operation Alice (investigation into the "plebgate" affair) and Kent Police's Operation Solar (relating to the trial of former minister Chris Huhne and his wife for perverting the course of justice). The Press Gazette and the National Union of Journalists (NUJ) launched the 'Save our Sources' campaign setting out their concerns and initiated a petition to the Commissioner.[3]

3.4 On 6th October 2014 the Commissioner decided to launch an inquiry into the use of powers under the Act to acquire communications data relating to the confidential sources of journalists as he shared the concerns raised relating to the protection of journalistic sources so as to enable a free press (see **Annex A page 38** for the statement issued by the interim Commissioner at that time).

[1] http://curia.europa.eu/juris/document/document.jsf?docid=150642&mode=req&pageIndex=1&dir=&occ=first&part=1&text=&doclang=EN&cid=228772
[2] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/331106/DRIPgovernmentNoteECJjudgment.pdf
[3] http://www.pressgazette.co.uk/save-our-sources-press-gazette-campaign-stop-uk-public-authorities-secretly-obtaining-journalists

4. Inquiry requirement for information and methodology

4.1 Section 58(1) of the Act imposes a statutory obligation on everyone concerned with Part 1 of the Act to disclose or provide all such documents or information to the Commissioner as he may require for the purpose of enabling him to carry out his functions under section 57.

4.2 On 6th October 2014 the Commissioner directed all police forces within the United Kingdom, under section 58(1) of the Act, to provide all such information and documents as the Commissioner required to conduct the inquiry (see **Annex B page 39-41** for the specific requirement). In brief the Commissioner required copies of the applications for communications data submitted in the past 3 years where the intention was to investigate the leaking of information to a journalist.

4.3 Importantly the requirement for information was not restricted to the communications addresses of journalists or the organisations they work for but went wider and included any communications data acquired on any communications address that sought to prove contact between a journalist and a public official with a view to identifying a journalistic source. The inquiry was not limited to the actions of those police forces reported in the media. Limiting our inquiry only to those actions or, only to the communications addresses of journalists would, in our view, have filtered out much of what we required to carry out a thorough examination of the processes and the extent to which the powers have been used for this purpose.

4.4 The requirement for information spanning three years was considered appropriate as we are aware of the archives police forces maintain in relation to applications for communications data and this would also cover the period of time that included the investigations highlighted in the media.

4.5 Copies of the applications and the considerations of the designated persons meeting the criteria outlined in the above mentioned letter were provided to the Commissioner. The applications specified the reasons for the investigation and what communications data had been sought. All of the police forces prioritised the requirement for information and responded within or shortly after the deadline of 13th October 2014. It is important to make clear that at present there is no requirement for public authorities to record the occupation of the person to whom the application relates (if that is indeed known at the time the application is made) or to hold a central record of investigations meeting the criteria of our inquiry. As such the steps that the police forces took to identify the relevant investigations should be described as best endeavors. On this point the new statistical requirements contained in the revised draft Code should enable such applications to be more easily identified in future.

4.6 We have not received separate briefings from the police forces to justify their investigations, although we have sought to clarify certain points and also required the police forces to identify the outcomes for the investigations that we deemed to be relevant. There were several requests from forces for guidance as to whether information in their possession met our requirements. **Annex C** (pages 42-44) provides detail in relation to the information that was excluded from the inquiry and the reasoning for the material's exclusion.

4.7 During our examination of submissions for this inquiry and the drafting of this report, consideration has had to be given to the fact that criminal investigations and legal proceedings are, within the meaning of the Contempt of Court Act 1981, invariably active. Taking full account of this does not mean that it is inappropriate to consider and make comment, as a matter of generality, the extent to which powers under Chapter 2 of Part 1 of the Act have been used and whether they were used appropriately. We have however chosen not to give our opinion as to the appropriateness of individual investigations in this report.

5. Engagement with journalists, the Association of Chief Police Officers (ACPO) and subject matter experts

5.1 In an effort to develop a better understanding of the underlying issues and concerns the inquiry team attended a one day conference hosted by the National Union of Journalists (NUJ) on the 16th October 2014. The conference ("Journalism in the age of surveillance: safeguarding journalists and their sources") considered the *chilling effect* caused by the police seeking out confidential journalistic sources. Several journalists, both speakers and those making interventions to contribute in the debate that followed, made explicit their outrage at the attempts of the police to identify their sources by acquiring communications data. They considered it to be an erroneous use of powers under the Act showing scant regard for the protections afforded to their sources within Article 10 of the Convention, the various statutes within the UK and, in particular, relevant case law. Those concerns were further articulated in the Press Gazette and NUJ 'Save our Sources' petition which was handed to IOCCO.

5.2 The Association of Chief Police Officers (ACPO) has various working groups that develop national standards. The inquiry team met with the national policing lead to the Counter Corruption Advisory Group within the ACPO National Policing Professional Standards and Ethics Portfolio to develop a better understanding of the issues currently being addressed by chief officers when police officers and / or police staff are suspected to have abused their authority which involves their committing a criminal offence. This includes leaking sensitive personal data or classified information to journalists. As we will outline later in this report the majority of the investigations examined as part of this inquiry related to such offences.

5.3 The inquiry team was also greatly assisted by Professor Anne Flanagan, Professor of Communications Law at Queen Mary University of London. Professor Flanagan kindly gave up her time to discuss issues, highlight concerns and assisted the inquiry team to develop some areas to consider in more detail. The professor's

published paper "*Defining journalism in the age of evolving social media: a questionable legal EU test*[4]*"* assisted the inquiry team's understanding of, for example, "journalism" in the modern media environment which has democratised the ability to publish to the point that many activities may come under the banner of 'citizen journalists.' The inquiry team asked the professor to consider how she would present information to police officers to assist them to understand better the varying interests at stake, such as freedom of expression, when investigating crimes in which a journalist may be a victim, a witness or a suspect. The latter would include circumstances where the journalist was suspected of crime connected with "journalism" and those which were not. Professor Flanagan produced a paper in this respect and has agreed its publication - See **Annex D** (pages 45 to 48) - *Proposed Guidance for Officers Considering a Request for Journalists Communications Data under RIPA 2000.*

[4] See A. Flanagan, 'Defining 'journalism' in the age of evolving social media: a questionable legal EU test' *Int J Law Info Tech (Spring 2013) 21 (1): 1-30.*

6. Review of the relevant law and policies

6.1 This inquiry is principally concerned with the acquisition of communications data by police forces under Chapter 2 of Part 1 of the Act to investigate criminal conduct by public officials constituting the leaking of information to the press. The acquisition of communications data in such cases is likely to reveal journalistic sources. As such the Act cannot be considered on its own as, although it permits communications data to be acquired in relation to criminality, other law and policies, such as Article 10 of the European Convention on Human Rights ("the Convention"), are relevant when data is sought to identify a journalist's source.

6.2 This section sets out the law within the Act and provides an analysis of other relevant law and policies relating to the protection of journalistic sources and access to records that directly identify journalistic sources and, considers key issues such as the right to freedom of expression, public interest and the so called *chilling effect* on sources willingness to provide information.

Chapter 2 of Part 1 of the Regulation of Investigatory Powers Act ("the Act")

6.3 There are strict rules governing who can obtain communications data and the circumstances in which they can access the data retained by Communication Service Providers (CSPs) and they are defined in Chapter 2 of Part 1 of the Act and the Code.

6.4 Communications data colloquially embrace the 'who', 'when' and 'where' of a communication but not the content, what was said or written. Put shortly, communications data comprise the following –

- *Traffic data* which is 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, and other related material (see sections 21(4)(a) and 21(6) and (7) of the Act and Paragraphs 2.19 to 2.22 of the Code).

- *Service use information* which is data relating to the use made by any person of a communication service and may be the kind of information that habitually used to appear on a Communications Service Provider's (CSP's) itemised billing document to customers (see section 21(4)(b) of the Act and Paragraphs 2.23 and 2.24 of the Code).
- *Subscriber information* which is data held or obtained by a CSP 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. For example, the recorded name and address of the subscriber of a telephone number or the account holder of an email address. (See section 21(4)(c) of the Act and Paragraphs 2.25 and 2.26 of the Code).

6.5 The giving of lawful authority for acquiring communications data is undertaken by a senior designated person within the public authority acquiring it. Under the Act and the Code there has to be;

- **an applicant**, a person who wants to acquire the communications data for the purpose of an investigation. The applicant has to complete an application form. The application must provide in structured form the details required by paragraph 3.5 of the Code.
- **a designated person**, is a person holding a prescribed office in the relevant public authority, who must decide whether it is lawful, necessary and proportionate to acquire the communications data to which the application relates. Their function and duties are described in paragraphs 3.7 to 3.14 of the Code. Except where it is unavoidable or for reasons of urgency or security, the designated person should not be directly involved in the relevant investigation.
- **a single point of contact (SPoC)** who is an accredited individual or group of accredited individuals trained to facilitate lawful acquisition of communications data and effective co-operation between a public authority and CSPs. Their functions are described in paragraph 3.15 to 3.21 of the Code.

- **a senior responsible officer (SRO)** within the public authority, who is responsible for the integrity of the process within that public authority to acquire communications data and for compliance with the Act and the Code.

6.6 **Necessity.** The mechanism by which a designated person may give authority to obtain communications data requires that person to believe that it is *necessary* to obtain it for one or more of the statutory purposes set out in section 22(2) of the Act. For police forces the purposes are -

- *in the interests of national security;*
- *for the purpose of preventing or detecting crime or of preventing disorder;*
- *in the interests of the economic wellbeing of the United Kingdom;*
- *in the interests of public safety;*
- *for the purpose of protecting public health;*
- *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 such; or*
- *for any purpose (not falling within the above which is specified for the purpose of this subsection by an order made by the Secretary of State).*

6.7 The vast majority of communications data are acquired for the purpose of *"preventing or detecting crime or of preventing disorder*[5]*."* Detecting crime is defined at section 81(5) of the Act and includes establishing by whom, for what purpose, by what means and generally in what circumstances any crime was committed, the gathering of evidence for use in any legal proceedings and the apprehension of the person (or persons) by whom any crime was committed. In relation to the investigation of crime, the Act does not restrict the acquisition of communications data to serious crime which is defined at section 81(2) and (3) of the Act.

6.8 It is therefore unhelpful when the reports in the media misinform the public by stating the use of powers to acquire communications data for crimes, not deemed to be of a serious nature under the Act, are inappropriate. It is also wrong for the

[5] 76.9% of communications data requests in 2013 were submitted for the purpose of preventing disorder or preventing or detecting crime - See Figure 7, Page 26 http://www.iocco-uk.info/docs/2013%20Annual%20Report%20of%20the%20IOCC%20Accessible%20Version.pdf

reports in the media to cite the Act as a terrorist law and infer that its use for non terrorist related matters is inappropriate.

6.9 **Proportionality.** A designated person is forbidden from approving an application for communications data unless he believes that obtaining the data in question, by the conduct authorised or required, is proportionate to what is sought to be achieved by so obtaining the data (see section 22(5) of the Act). Thus every application to acquire communications data has to address proportionality explicitly. This involves balancing the extent of the intrusiveness of the interference against a specific benefit to the investigation or operation being undertaken by a relevant public authority in the public interest. He or she must also believe that conduct is no more than is required in the circumstances. Any conduct that is excessive in the circumstances of both the interference and the aim of the investigation or operation, or is in any way arbitrary will not be proportionate.

6.10 Chapter 2 of Part 1 of the Act appears to provide an exclusive scheme whereby communications data can be obtained. This is reinforced by section 21(1) which states that the Chapter applies to 'any conduct' in relation to obtaining of communications data, and to the disclosure to 'any person' of such data. The approach appears consistent with paragraph 1.3 of the Code which states [emphasis added] -

> *"Relevant public authorities for the purposes of Chapter 2 of Part 1 of the Act should not:*
>
> - *Use other statutory powers to obtain communications data from a postal or telecommunications operator unless that power provides explicitly for obtaining communications data, or is conferred by a warrant or order issued by the Secretary of State or a person holding judicial office, or*
>
> - *Require, or invite, any postal or telecommunications operator to disclose communications data by exercising any exemption to the principle of non-disclosure of communications data under the Data Protection Act 1998."*

6.11 In plain language that means public authorities should not use other laws to obtain communications data from a CSP unless that law provides explicitly for obtaining communications data.

6.12 Parliament recently reinforced those restrictions within the Data Retention and Investigatory Powers Act (DRIPA) 2014 at section 1(6)(a) which puts a duty on the CSP not to disclose communications data retained as a result of a requirement within section 1 of DRIPA unless it is a requirement made under Chapter 2 of Part 1 of the Act; or a court order or other judicial authorisation or warrant.

6.13 The Police and Criminal Evidence Act 1984 (for example section 9 and schedule 1) does not have a specific provision requiring the disclosure of communications data to the police or to the courts.

6.14 There has been a misunderstanding in the media as regards to the appropriate use of production orders such those described at section 9 and schedule 1 of PACE. Several media reports claimed that the police, when acquiring communications data under the Act, had circumvented the process of judicial approval for such an order and that a journalist, ordinarily, is able to attend a hearing and put forward submissions opposing the order if it is appropriate to do so. This understanding of practice is likely to arise as the police will often seek access to journalistic material to investigate crime by seeking a production order (for example, unedited film footage capturing the commission of a crime in action or seeking the origin of a story which may impact a crime investigation). The order, if granted by a judge, will require the disclosure of the material held by the journalist or the media company they work for. If the journalist or their legal representative wishes to oppose a judge granting an order or make submissions restricting the scope of an order they would have the opportunity to do so at the *inter partes* hearing.

6.15 The assertion that the police circumvented judicial approval and denied a journalist the opportunity to have a draft order set aside when seeking the disclosure of communications data retained by a CSP is arguably flawed for several reasons –

- PACE (section 9 and schedule1) does not have a specific provision requiring the disclosure of communications data to the police or to the Courts;
- Even if the police sought a production order under PACE to acquire communications data -
    - the schedule 1 notice and draft order are served on the holder of the data (the CSP retaining the data) and not the person who may be subject of the investigation; and
    - if the draft order is to be opposed the *inter partes* hearing would be attended by the applicant (the police), the holder of the data (the CSP retaining the data) and the judge but not the person who may be the subject of the investigation.

6.16 Communications data generated and processed by CSPs are business records. They do not contain any details of what was said or written by the sender or the recipient of the communication. As such, the communications data retained by CSPs do not contain any material that may be said to be of professional or legal privilege – the fact that a communication took place does not provide what was discussed or considered or advised. However, it may be possible from the acquisition and analysis of communications data to infer that an issue of sensitivity is under consideration because a person has regular contact with, for example a lawyer, doctor, journalist, Member of Parliament, or minister of religion and this is the key point.

6.17 The Home Office published a revised Code for the acquisition of communications data for public consultation[6] in December 2014 after outlining in July

[6] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/383548/DraftCDAcquisitionCodeofPracticeforconsultation.pdf

2014 the Government's intention to amend the code. The revised draft Code states in Paragraphs 3.72 to 3.74 that –

> *"The degree of interference may be higher where the communications data being sought relates to a person who is a member of a profession that handles privileged or otherwise confidential information (such as a medical doctor, lawyer, journalist, Member of Parliament or minister of religion). It may also be possible to infer an issue of sensitivity from the fact that someone has regular contact with, for example, a lawyer or journalist.*
>
> *Such situations do not preclude an application being made. However applicants, giving special consideration to necessity and proportionality, must draw attention to any such circumstances that might lead to an unusual degree of intrusion or infringement of privacy, and clearly note when an application is made for the communications data of a medical doctor, lawyer, journalist, Member of Parliament, or minister of religion. Particular care must be taken by designated persons when considering such applications."*

6.18 The current and revised Codes do not provide any clear guidance on how designated persons should actually apply the principles of necessity, proportionality and collateral intrusion when dealing with data relating to communications with journalists or take account of the added dimension that the requirement may lead to the identification of journalistic sources, whether an intended consequence or not. As such the law governing freedom of speech and the protection of journalistic sources must also be considered. The next section will explore such issues along with some of the law and policies governing investigations into criminal conduct by public officials.

Article 10 of the European Convention on Human Rights ("the Convention") and law relevant to freedom of speech and protecting journalistic sources

6.19 The need to protect the confidentiality of journalistic sources is crucial to safeguard the free press in a democratic society. It is a protection that depends heavily on Article 10 of the European Convention on Human Rights ("the Convention"). Article 10 of the Convention - the right to freedom of expression - is a qualified right, in other words it can be interfered with to achieve a balance with other fundamental rights. The circumstances in which freedom of expression can be restricted are set out in sub-paragraph (2) of Article 10 -

> *"The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary."*

6.20 The Contempt of Court Act 1981, at section 10, was introduced by the Government in response to the European Court of Human Rights (ECHR) ruling within *Sunday Times v United Kingdom*[7] -

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

6.21 The Leveson Inquiry[8] highlighted the need to protect the confidentiality of journalistic sources who provided information with an expectation of confidence –

[7] (1979) 2 EHRR 245 –see http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-57584#{"itemid":["001-57584"]}
[8] See Volume 1 – Part B – Chapter 2 Para 6.1 p68 - The protection of sources and other legal privileges of the press https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/270939/0780_i.pdf

> *A free press is able to perform valuable functions which individual free speech cannot. It is because of the position of the press as an institution of power that it is able to stand up to and speak truth to power. The professional skills and resources at its disposal enable the press as an institution to carry out ground-breaking investigations in the public interest. It is these considerations and functions which have resulted in the press as an institution being afforded certain privileges going beyond those protected by freedom of speech.*

6.22 The press privilege not to disclose sources of information, within section 10 of the Contempt of Court Act 1981, means that a publisher cannot be compelled to reveal the source of published information unless a court considers such disclosure to be in the interests of justice or national security or for the prevention of crime.

6.23 The Police and Criminal Evidence Act (PACE) 1984 has similar procedural privilege, preventing the police from access to journalistic material without an order granted by a judge. Furthermore, the courts have also recognised the right not to disclose sources as an important facet of the free press, as is reflected in the following words of Lord Woolf CJ[9] -

> *"The fact that journalists' sources can be reasonably confident that their identity will not be disclosed makes a significant contribution to the ability of the press to perform their role in society of making information available to the public."*

6.24 Nevertheless, the laws in the United Kingdom retain the power for the courts to compel journalists to reveal their sources when it relates to one of the purposes set out in Article 8 and 10 of the Convention (for example for the prevention of disorder or crime).

6.25 Emmerson and Friedman (1998)[10] comment that the protection given by section 10 of the Contempt of Court Act 1981 has not always been found sufficient to

[9] See *Ashworth Hospital Authority v MGN Ltd* [2002] 4 All ER 193, 210.
[10] Emmerson, B. QC., and Friedman, D. QC., A Guide to the Police Act 1997 (1998) Butterworths, (London) – p66 – 67.

satisfy Article 10 of the Convention[11]. However, section 10 creates a strong presumption in favour of protecting journalistic sources and places a heavy burden on a party seeking disclosure to displace the presumption. In *Secretary of State for Defence v Guardian Newspapers*[12] a copy of a classified document concerning the arrival of cruise nuclear missiles at Greenham Common (US Air Force base) was leaked to The Guardian, which published it. The Ministry of Defence sought an order for recovery of the document in order to identify the source of the leak. The House of Lords ruled that the protection afforded by section 10 applied, so as to place a burden on the party seeking disclosure to show that it was necessary for one of the statutory purposes, and not merely expedient.

6.26 Measures creating a *chilling effect* on freedom of expression have been held to breach the Convention. In *Goodwin v United Kingdom*[13] the ECHR laid down the following principle on the application of Article 10 –

> *"The Court recalls that freedom of expression constitutes one of the essential foundations of a democratic society and that the safeguards to be afforded to the press are of particular importance. 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. As a result the vital public watchdog role of the press may be undermined and the ability of the press to provide accurate and reliable information may be adversely affected. Having regard to the importance of the protection of journalistic sources for the press freedom in a democratic society, and the potentially* ***chilling effect*** *an order of source disclosure has on the exercise of that freedom, such a measure cannot be compatible with Article 10 of the Convention, unless it is justified by an overriding requirement in the public interest."*

6.27 The debates within Parliament concerning confidential material resulted in safeguards being included into the Police Act 1997 that dealt with matters subject to

[11] See for example Goodwin v United Kingdom (1996) 22 EHRR 123 http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-60596#{"itemid":["001-60596"]}
[12] [1985] 1 AC 339, [1984] 3 All ER 601, HL.
[13] See also *Jersild v Denmark* (1994) 19 EHRR 1 http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-57891#{"itemid":["001-57891"]}

legal privilege, confidential personal information and confidential journalistic material (see sections 98, 99 and 100).

6.28 The wording of section 100 of the Police Act 1997 can be compared with section 13 of the Police and Criminal Evidence Act 1984 (PACE). Emmerson and Friedman (1998) argue that PACE also affords special protection to this type of material which provides considerably greater protection than the Police Act 1997. Section 14 of PACE provides that ordinary searching procedures are not to have effect in relation to journalistic material (other than material excluded under section 11 of PACE) and creates special procedures for obtaining a warrant from a circuit judge. Where the journalistic material qualifies as 'confidential', it is immune from an ordinary search warrant and the interested party has a right to be heard before an order is made[14].

6.29 Emmerson and Friedman (1998) argue that the Police Act 1997 provides a means by which the police can gain access to confidential journalistic material which is not available to them under PACE and that the Police Act 1997 *"undoubtedly has the potential to give rise to violations of Article 10 of the European Convention of Human Rights."* The Regulation of Investigatory Powers Act 2000 ("the Act") came into force a number of years later and the observations of Emmerson and Friedman (1998) appear pertinent to it when reviewing its use to identify journalistic sources.

6.30 This consideration is amplified by *Recommendation No R (2000) 7 of the Committee of Ministers to Member States*[15]. We therefore take the view that actions to identify journalistic sources will include –

- requirements made directly to the journalist or their employer to disclose the identity of their source which may include legal proceedings;
- the acquisition of communications data relating to the journalist; employers of the journalist; person or persons suspected of being the

[14] See section 9 and schedule 1 (paragraph 7) of PACE
[15] See Council of Europe Committee of Ministers https://wcd.coe.int/ViewDoc.jsp?id=342907&Site=CM

journalist's source; an intermediary; a person acting for the journalist, their source or for both the journalist and the source.

6.31 The term "journalist"[16] for the purposes of this inquiry means any natural or legal person who is regularly or professionally engaged in the collection and dissemination of information to the public via any means of mass communication. Professor Anne Flanagan explained the term "journalism" as-

> *"The gathering, verification and dissemination of news and other information that the public needs in their daily lives and to participate as citizens. Whether those that engage in journalism are paid or work for traditional media organisations is irrelevant. Also irrelevant is the technology or format used.*[17] *What is key to distinguishing journalism or expression entitled to the enhanced safeguards from other kinds of communications is whether it meets two criteria: the content should meet a threshold public interest test; it should also be accurate and reliable under journalism standards."*

6.32 Our analysis now considers matters in more detail where the interference is with a person's rights under Article 10 relating to identifying a journalist's source. The matter that needs to be considered in the first instance is whether the public interest is, on the one hand, in the publication of the leaked material or whether, on the other hand, the public interest leans towards the police identifying and then seeking to prosecute the journalist's source. In setting the context to this issue, Dr Mawby (lecturer in criminology at the University of Leicester) suggested in his evidence to the Leveson Inquiry[18] that -

> *"… unauthorised disclosures or "leaks" by police personnel to the media will always be a threat to a police force's control of information to a greater or lesser degree depending on circumstances. The disgruntled employee or the whistle blower can be an important media source. The extent to which leaks are either in the public interest (for example, bringing malpractice to light) or a*

[16] See the Appendix to the Recommendation No R (2000) 7 of the Committee of Ministers to Member States at https://wcd.coe.int/ViewDoc.jsp?id=342907&Site=CM

[17] Journalism often uses social media forms appropriate to the situation which may serve as helpful examples here. See, eg,'Peter Jukes is named best UK Reporter on Twitter and social media – full Press Gazette top 50 list', Press Gazette (8 April 2014), http://www.pressgazette.co.uk/peter-jukes-named-best-uk-reporter-twitter-and-social-media-full-press-gazette-top-50-list ; L. Oberst, 'Journalism and Social Media: 15 Examples Worth Learning From', Centre for Sustainable Journalism (26 Oct 2011), http://sustainablejournalism.org/socialmedia/journalism-social-media-examples.

[18] See http://www.levesoninquiry.org.uk/wp-content/uploads/2012/04/Witness-Statement-of-Dr-Rob-Mawby.pdf page7

problem (for example, putting someone in danger) depends on the circumstances of each incident."

6.33 As a starting point, Professor Anne Flanagan[19] provided the following summary of *public interest* where it relates to publishing information -

"The greater the public interest in publishing or receiving certain information or expression, the more likely that it will be subject to enhanced protection under the right to freedom of expression, even where it is uncertain that it comprises 'journalism' as such. What information or expression is in the public interest is not the same as whether it is interesting to the public.

Public interest in information or expression instead relates to its need and value in the lives of people and their ability to participate in a democratic society. There is no set or finite list of information or expression that is in the public interest to publish or receive. If however there were a sliding scale of public interest, issues like the conduct of government (national and local) and matters concerning politics would likely be considered as having the greatest public interest. Information on topics like finance, health, religion, science, crime, national security, culture and the arts are also likely to have a high level of public interest. At the other end of the scale, mere 'tittle tattle', gossip and tawdry details about personal lives are likely to have a much lower level of public interest.

So, if a publication addresses issues with a greater public interest factor like political speech, this should get greater weight in the balancing of interests as to whether an intrusion on the journalist's freedom of expression might be justified."

6.34 In cases that have been before the courts seeking to identify a journalist's source judicial opinion seems to vary as to the relevance of, or weight that can be given to, the public interest in the information provided in determining whether to order revelation of the source.

6.35 In *X Ltd v Morgan Grampian Publishers*[20] (House of Lords - 1991) Lord Bridge finds that judges should undertake a balancing exercise where one of the possibly

[19] See Annex D of this report (pages 45 to 48)
[20] See http://www.publications.parliament.uk/pa/ld200102/ldjudgmt/jd020627/ash-2.htm

relevant factors is the 'legitimate interest in the information'. Similarly in Financial Times Ltd. & Ors v Interbrew SA[21] (Court of Appeal - 2002) Lord Justice Sedley states –

> *".....The purpose of the leak.....is likely to be highly material. If it is to bring wrongdoing to public notice it will deserve a high degree of protection....."*

6.36 This seems contrary to Lord Justice Laws' judgment in *Ashworth Security Hospital v MGN Limited*[22] (Court of Appeal - 2000):

> *".....The public interest in the non-disclosure of press sources is constant, whatever the merits of a particular publication, and the particular source....."*

6.37 Lord Justice Sedley's judgment indicates that consideration should be given to whether the information provided by the source has public interest value, whereas Lord Justice Laws' judgment suggests it is actually an irrelevance.

6.38 Whichever way the public interest leans, the concerns expressed in the media which led to this inquiry being launched highlight the *chilling effect* or collateral impact that occurs when a journalist is required to disclose the identity of a source to the court. The effect is arguably the same when the police use their powers under the Act to acquire communications data to identify a journalist's source through analysis of that data.

6.39 Thus, even though the requirement to identify the source may appear, taking account of the requirements of Article 10, legitimate in order to investigate a serious crime or address matters relating to national security, the *chilling effect* or collateral impact is ever present.

6.40 It is therefore inevitable that a complex argument should develop when Article 10 and the accompanying case law is properly considered when setting out the justifications to identify a journalist's source. In this context consideration should be

[21] See http://www.bailii.org/cgi-bin/markup.cgi?doc=/ew/cases/EWCA/Civ/2002/274.html&query=interbrew&method=boolean
[22] See http://www.bailii.org/cgi-bin/markup.cgi?doc=/ew/cases/EWCA/Civ/2000/334.html&query=rougier+and+j&method=boolean

given to *Recommendation No R (2000) 7 of the Committee of Ministers to Member States*[23] on the right of journalists not to disclose their sources of information and the point at which it may be appropriate for the state (for example, the police) to interfere with the Article 10 rights by the appropriate use of investigatory powers.

6.41 The Crown Prosecution Service (CPS)[24] has acknowledged that *Recommendation No R (2000) 7* is not legally binding but is of assistance in interpreting and applying the rights and guarantees of the Convention itself including Article 10. Principle 6 (Interception of communication, surveillance and judicial search and seizure) provides as follows [emphasis added] -

> *a. The following measures should not be applied if their purpose is to circumvent the right of journalists, under the terms of these principles, not to disclose information identifying a source:*
>
> *i. interception orders or actions concerning communication or correspondence of journalists or their employers,*
>
> *ii. surveillance orders*[25] *or actions concerning journalists, their contacts or their employers, or,*
>
> *iii. search or seizure orders or actions concerning the private or business premises, belongings or correspondence of journalists or their employers or personal data related to their professional work.*
>
> *b. Where information identifying a source has been properly obtained by police or judicial authorities by any of the above actions, although this might not have been the purpose of these actions, measures should be taken to prevent the subsequent use of this information as evidence before courts, unless the disclosure would be justified under Principle 3.*

6.42 Principle 3 (cited in Principle 6) acknowledges, in relation to Article 10 of the Convention*, where there exists an overriding requirement in the public interest and if circumstances are of a sufficiently vital and serious nature.*

[23] See https://wcd.coe.int/ViewDoc.jsp?id=342907&Site=CM
[24] See Prosecuting Cases Where Public Servants Have Disclosed Confidential Information to Journalists at http://www.cps.gov.uk/legal/p_to_r/prosecuting_cases_where_public_servants_have_disclosed_confidential_information_to_journalists/
[25] See section 48(1) & (2)(a) of the Regulation of Investigatory Powers Act 2000 – "surveillance" includes monitoring, observing or listening to persons, their movements, their conversations or their other activities or communications

6.43 The CPS summarise[26] the legal protections for journalistic sources as follows -

The Convention, various statutes, European and United Kingdom case law all make it clear that:

- *freedom of expression is one of the most important rights in the Convention;*
- *any restriction on that right must be necessary in democratic society, which in turn requires that:*
    - *it has a legitimate aim, such as the prevention of crime or the protection of the rights of others, as set out in Article 10(2);*
    - *the aim must reflect a 'pressing social need', i.e. be sufficiently important to justify the restriction;*
    - *the restriction must be rationally related to that aim; and*
    - *a fair balance must be struck between the rights of the individual and the general interest of the community;*
- *the necessity for the restriction must be convincingly established in view of the importance of freedom of expression. The domestic courts must apply the principle of proportionality in this way under the HRA: see* Huang v Secretary of State for the Home Department [2007] 2 AC 167, *paragraph 19.*

6.44 The consequence, according to the CPS, for investigators and prosecutors is that, in cases which rely on the disclosure of journalistic sources or on covert techniques which involve or amount to the revealing of a source's identity, the prosecution will have to satisfy the court that the admission of evidence that reveals the identity of a journalistic source is exceptionally required by a pressing social need and that it is proportionate in the circumstances of the case. This can be done in appropriate cases but, in discharging this burden, the prosecution will have to rebut the presumption that it is always prima facie contrary to the public interest that press sources should be disclosed. Expressed another way, there is an underlying assumption that it is not in the public interest to identify a journalist's source.

[26] See Prosecuting Cases Where Public Servants Have Disclosed Confidential Information to Journalists at http://www.cps.gov.uk/legal/p_to_r/prosecuting_cases_where_public_servants_have_disclosed_confidential_information_to_journalists/

6.45 The CPS guidance (published 2009) concludes that in cases involving journalists, Principle 6 would appear to rule out many of the normal covert techniques. However, the prohibition is not absolute. Principle 6 refers to, and thus adopts, the same exception as Principle 3 which contemplates the possibility that there may be cases where overriding requirements of the public interest make it necessary to interfere with the general right of a journalist to keep sources confidential [emphasis added] –

> *"The joint effect of Recommendation 7 and Article 10 (which is the primary source), is that* ***very important factors will be required to outweigh the general right of a journalist to keep sources confidential****. It is therefore important that offences are not investigated in ways which are contrary to Principle 6, unless the circumstances are sufficiently serious and vital to warrant this".*

6.46 This indicates that prosecution or even a criminal investigation should be seen as a last resort reserved for the most serious of cases. If that is done, investigations and prosecutions are more likely to be held to be compatible with Article 10. Such situations, therefore, do not preclude the acquisition of communications data within a sufficiently serious criminal investigation where very important factors are present in sufficient quantity so as to justify identifying a journalist's source.

6.47 In conclusion Chapter 2 of Part 1 of the Act appears to provide an exclusive scheme whereby communications data can be obtained. This is reinforced by section 21(1) which states that the Chapter applies to 'any conduct' in relation to obtaining of communications data, and to the disclosure to 'any person' of such data. Where a public authority suspect wrongdoing constituting misconduct in public office they must consider properly whether that conduct is criminal and of a sufficiently serious nature for Article 10 rights to be interfered with where communications data is to be acquired for the purpose of identifying a journalist's source. In addition matters relating to actions seeking to identify a journalist's source need to show that it is

necessary for one of the statutory purposes and not merely expedient, and such a measure cannot be compatible with Article 10 of the Convention unless it is justified by an overriding requirement in the public interest.

6.48 We also considered publications by the Independent Police Complaints Commission (IPCC), Her Majesty's Inspectorate of Constabulary (HMIC), the Association of Chief Police Officers (ACPO), the College of Policing and Elizabeth Filkin[27] concerning the investigation of police corruption, misconduct in public office and leaks to the press. A summary of these publications is contained in **Annex E** (pages 49 to 55)**.** The publications considering 'leaks to the press' and 'undeclared relationships with the press' put emphasis that a low threshold will apply to the point that a state of zero tolerance appears, in practice, to be operating. Little reference, if any, is made to Article 10 of the Convention or the published guidance from the CPS. Consequently, the publications by the IPCC, ACPO, College of Policing, HMIC and Filkin must not be considered in isolation by chief officers especially if the police are seeking to embark on investigations to identify who within an organisation has leaked information to the media.

[27] http://webarchive.nationalarchives.gov.uk/20140122145147/http:/www.levesoninquiry.org.uk/wp-content/uploads/2012/03/Report-by-Elizabeth-Filkin.pdf

7. The nature and extent of the use of the powers under the Act

Statistical Information

7.1 In the 3 year period covered by the inquiry 19 police forces reported undertaking 34 investigations which sought communications data in relation to suspected illicit relationships between public officials (sources) and journalists. The 34 investigations concerned relationships between 105 journalists and 242 sources[28].

7.2 608 applications under Chapter 2 of Part 1 of the Act were authorised to seek this communications data. This represents an extremely small percentage (0.1%) of the total applications that were authorised by the police in that 3 year period.[29]

7.3 Commonly the investigations were internal Police Professional Standards[30] enquiries concerned with the disclosure of information to journalists by police officers and police staff which was considered sensitive and therefore deemed to be a criminal act - typically misconduct in public office, a breach of data protection or an offence under the computer misuse act. Exceptionally they related to contempt of court and the offence of conspiracy to pervert the course of justice.

7.4 The Metropolitan Police Service's (MPS's) Operation Elveden was notable amongst the 34 investigations for three reasons. First, it is concerned with illicit leaks from a wider range of public officials in addition to police officers and staff. **Figure 1** (over page) provides the professions for the 34 investigations. Second, Operation Elveden accounted for 484 (80%) of the 608 applications which sought communications data. To provide context to the usage, removing this exceptional operation from the overall statistics would represent less than 1 application per

[28] 242 represents the maximum number of sources - there is likely to be duplication because at the time an application is submitted the source may not have been identified but they may later be revealed as a source that data had already been acquired in relation to.
[29] Approximately 0.1% of the 500,000 applications estimated to have been submitted in the 3 year period by police forces. NB - the 500,000 application figure is based on a ratio of an average of 2.5 notices and authorisations to one application.
[30] This is the common title given to departments within police forces that undertake investigations concerning criminal or malpractice allegations concerning members of the organisation.

police force per year (when averaged out over the 3 years and all the UK police forces).[31]

Figure 1 - Professions of suspected journalist sources in the 34 police investigations

Source Profession	Number of Sources
Police Officer / Police staff	126
Prison Officer / Secure Hospital staff	52
Military staff	38
Central / Local Government staff	4
Other or unspecified / unknown	22

7.5 Third, Operation Elveden is atypical as the initial reason for suspecting there was a corrupt public official working with a journalist came in the vast majority of cases from the material disclosed to the MPS by the News International Management Standards Committee (MSC)[32] (for example, emails and financial records), or from devices or material seized from journalists as the investigation continued (for example, downloads from mobile phones seized from journalists or entries made within their notebooks). This has already been commented upon in **Annex C** (pages 42-44).

7.6 The journalists of interest to the 34 police investigations were mainly from national, regional or local newspapers. There was also a small number of freelance, broadcast and new media, e.g. bloggers (see **Figure 2**).

Figure 2 - Type of journalist in the 34 police investigations

Journalist Type	Number of Journalists
National newspaper	69
Regional / Local newspaper	19
Freelance	7
Broadcast	3
New media	1
Unknown / unspecified	6

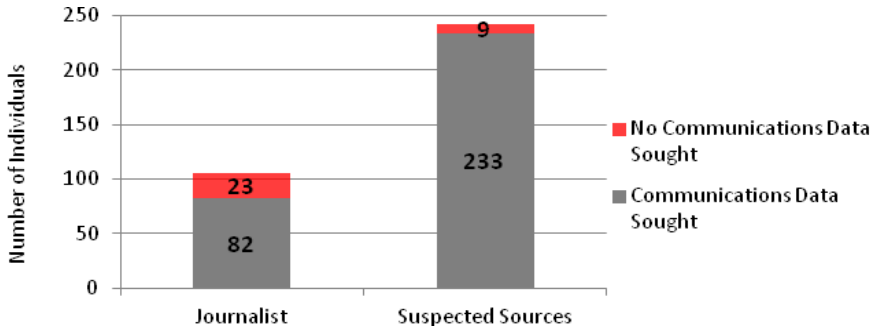
[31] 124 applications, divided by 46 UK police forces, divided by 3 year period of the inquiry.
[32] See more information re the MSC in Annex C of this report.

7.7 The 34 police investigations sought communications data on 233 (96%) of the 242 suspected illicit sources (see **Figure 3**).

7.8 24 of the 34 police investigations sought communications data on one or more of the journalists relevant to that investigation which equated to 82 (78%) of the 105 journalists (see **Figure 3**). The other 10 investigations did not seek data on any journalist i.e. they only sought communications data attributable to the source to help establish if there was an illicit relationship.

7.9 43% of the data sought on journalists was traffic or service use data, such as call data on phones (including 31 office landlines), typically for periods of 1 or 2 months. From an Article 10 perspective this type of data is potentially more sensitive and the legal issues are more complex than subscriber data, or data relating to devices used by a journalist's source, because it can ultimately be used to identify numerous sources, including those that may not be relevant to the police investigation.

Figure 3 - Number of Journalists and Sources



Nature of the investigations examined

7.10 The reasons for suspecting and initiating a criminal investigation concerning information being leaked or supplied to a journalist, based on our examination of the applications, were in the main initiated when the police force become aware that the journalist was in possession of or had access to information that is not available outside of the organisation or a particular investigation (and is considered to be

sensitive personal data or protected information from their internal or national information systems). The awareness of the information being in the possession of the journalist can be through –

- the journalist making an approach to the police (for example, their press office) indicating they have certain information;
- the publication of an article which contains information the police consider could only have been obtained through unlawful disclosure; and
- voluntary disclosure of information to the police indicating criminal conduct by a journalist (see for example matters relating to the MSC within **Annex C** pages 42 to 44).

7.11 The reasons public officials may wish to share or 'leak' sensitive confidential or other information with a journalist were varied and ranged from a desire to damage the reputational standing of that organisation; a desire to put into the public domain information about poor practice or misuse of funds; or receiving payment from journalists or persons claiming to be journalists seeking access to operationally sensitive information.

7.12 The type of information leaked included that relating to -

- expenditure e.g. impact of the austerity measures or what serving staff regarded as inappropriate use of expenditure by their seniors;
- information about crime investigations e.g. that a murder or other serious crime had occurred, the circumstances and the persons involved, positive DNA / fingerprint results naming the offender prior to their arrest;
- the specific manner in which a person had been raped or murdered with details of the weapon and / or their specific injuries;
- information about internal investigations against police officers and staff including allegations of theft, drinking on duty and sexual misconduct;
- information about high profile persons known to the media, notorious or celebrity prisoners, prison security issues etc.

Findings relating to the examination of the applications

7.13 We examined the applications with regard to the requirements within the Act, the Code and the law and policies applicable to identifying journalistic sources detailed in **section 6 (pages 11 to 28)** of this report.

7.14 All the applications were set out in a manner that conformed to the Act, the Code and the guidance published by the Home Office and ACPO Data Communications Group (DCG). All of the applications had been authorised by a designated person of the correct rank within the police force and specified the statutory purpose of preventing and detecting crime or preventing disorder (section 22(2)(b) of the Act).

7.15 The majority of applications did not sufficiently justify the principles of necessity and proportionality and required further information to justify why it was more important to identify the journalist's source than to respect their anonymity in the specific circumstances of the investigation. This included -

- a lack of specific detail about the information that had been (or was suspected to have been) leaked;
- whether in the circumstances of the case the high threshold for suspecting the common law offence of misconduct in public office had been met;
- insufficient consideration of whether the leaked information was of public interest merit;
- what actual damage the leaked information had caused, or was likely to cause;
- whether the damage caused by the provision of that information amounted to a pressing social need justifying identification (and perhaps sanction) of the source;
- whether there was a disproportionately high risk of collateral intrusion into legitimate journalistic sources, and;
- a lack of detail about how the data would be analysed, processed and retained within the public authority to prevent unwarranted intrusion.

7.16 The poor quality of many of the applications is in part due to the fact that the application process that has been designed by the Home Office and ACPO Data Communications Group (DCG) is focused on privacy considerations relevant to Article 8 of the Convention and provides no guidance or assistance relevant to Article 10 of the Convention.

7.17 The small minority of applications that were completed to a sufficient or high standard tended to have benefited from legal advice obtained from in-house lawyers or a prosecuting authority. In these cases the designated person considering the application was able to make a better assessment of the relevant issues and in several instances this had led to a refusal of the application.

Outcomes of the police investigations

7.18 Police forces were contacted to determine whether their investigations identified a suspect (i.e. the journalist's source) and, if so, was an advice file submitted to the prosecutor; whether anyone had been charged with an offence; and whether anyone had been dealt with by an internal discipline hearing. The following responses were received –

- 2 investigations are ongoing.
- 20 investigations resulted in no action.
- 5 investigations led to criminal charges against 68 individuals (of which Operation Elveden accounted for 64). Some of these prosecutions are ongoing.
- 4 investigations submitted an advice file to the prosecutor who decided not to bring charges.
- 10 investigations (including 2 of those where criminal charges were made) resulted in disciplinary action - 15 dismissals and 5 occasions where management advice was given.
- 3 investigations are planning disciplinary proceedings.

8 Conclusions and recommendations

8.1 In the 3 year period covered by the inquiry 19 police forces reported undertaking 34 investigations which sought communications data in relation to suspected illicit relationships between public officials (sources) and journalists.

8.2 608 applications under Chapter 2 of Part 1 of the Act were authorised to seek this communications data. This represents a very small percentage (0.1%) of the total applications that were authorised by the police in that period which demonstrates that such usage is not widespread. These figures are also artificially inflated by exceptional investigations like Operation Elveden[33] – removing that investigation from the overall statistics provides context and would represent less than 1 application per police force per year (when averaged out over the 3 years and all UK police forces).[34]

8.3 Police forces are not randomly trawling communications data relating to journalists in order to identify their sources. The applications examined in the main related to investigations where public officials were suspected of criminal conduct or where a media organisation had voluntarily disclosed information to the police relating to what they believed to be criminal conduct for investigation.

8.4 The acquisition of communications data is currently relevantly regulated by Chapter 2 of Part 1 of the Act and the Code (see Paragraphs 6.3 to 6.18 of this report). Police forces have not circumvented other legislation by using their powers under Chapter 2 of Part 1 of the Act to acquire communications data in these cases. However the observations of Emmerson and Friedman (1998)[35] set out earlier in this report appear pertinent to the acquisition of communications data when reviewing its use to identify journalistic sources, i.e. that it undoubtedly has the potential to give rise to violations of Article 10 of the Convention.[36]

[33] See Paragraph 7.4 of this report. Operation Elveden accounted for 80% of the 608applications.
[34] 124 applications, divided by 46 UK police forces, divided by 3 year period of this inquiry.
[35] Emmerson, B. QC., and Friedman, D. QC., A Guide to the Police Act 1997 (1998) Butterworths, (London) – p66 – 67.
[36] See Paragraphs 6.25 to 6.29 of this report.

8.5 Chapter 2 of Part 1 of the Act permits designated persons to authorise the acquisition of communications data which are necessary for preventing or detecting crime or preventing disorder (see section 22(2)(b) of the Act). Misconduct in public office is currently a sufficient crime to meet that test[37]. A designated person is forbidden from approving an application for communications data unless he believes that obtaining the data in question is proportionate to what is sought to be achieved (see section 22(5) of the Act).

8.6 We are not satisfied that generally speaking the applicants or designated persons in fact gave the question of necessity, proportionality and collateral intrusion sufficient consideration in the applications that we examined as part of this inquiry[38]. The applications focused on privacy considerations relevant to Article 8 of the Convention and did not give due consideration to Article 10 of the Convention.

8.7 The current Code and the revised draft Code (which seeks to address this point in Paragraphs 3.73 to 3.74) do not provide any specific guidance on how designated persons should actually apply the question of necessity, proportionality and collateral intrusion when dealing with data relating to sensitive professions, in particular journalists. The acquisition and subsequent analysis of data relating to communications with a journalist is likely to reveal journalistic sources and therefore general law relating to Article 10 of the Convention and the protection of journalistic privilege must be considered[39].

8.8 The question is whether it is sufficient to give designated persons generalised guidance only, or whether the power to authorise the acquisition of communications data which seriously risks revealing the confidential sources of journalists should be removed from those presently properly appointed as designated persons and passed by statute to a Judge. The reasons for this change would be that (a) the revised draft Code is not sufficient in giving clear and adequate guidance and, (b) our investigations

[37] Paragraphs 1.1 to 1.5 of Annex E are relevant to this offence.
[38] See Paragraphs 7.13 to 7.18 of this report.
[39] See in particular paragraphs 6.19 to 6.48 of this report.

indicate that applicants and designated persons do not in fact adequately address the principles which the Code should explain clearly. A judicial decision, such as legislation requires in other related circumstances, would necessarily address the legal considerations in full, in particular these questions with reference to the particular facts of the individual case.

8.9 After careful consideration of all the evidence we have collected and reviewed in this inquiry and due to the sensitivities and complexities of the considerations required when contemplating an interference with Article 10 of the Convention we make the following two recommendations -

1. *Judicial authorisation must be obtained in cases where communications data is sought to determine the source of journalistic information.*

2. *Where communications data is sought that does not relate to an investigation to determine the source of journalistic information (for example where the journalist is a victim of crime or is suspected of committing a crime unrelated to their occupation) Chapter 2 of Part 1 of the Act may be used so long as the designated person gives adequate consideration to the necessity, proportionality, collateral intrusion, including the possible unintended consequence of the conduct[40]. The revised Code contains very little guidance concerning what these considerations should be and that absence needs to be addressed.*

8.10 Our conclusion is to advise the Government to implement these recommendations in order to provide adequate protection for journalistic sources, and enhanced safeguards to prevent unnecessary or disproportionate intrusions.

[40] See Paragraphs 6.16, 6.18, 7.15 of this report - and - Annex C Paragraph 1.9.

Annex A

6th October 2014 - IOCCO Launches Inquiry into the use of RIPA powers to acquire communications data relating to the confidential sources of journalists

Today the Rt Hon. Sir Paul Kennedy, Interception of Communications Commissioner has launched an inquiry into the use of RIPA powers to determine whether the acquisition of communications data has been undertaken to identify journalistic sources. The Rt Hon. Sir Paul Kennedy says:

"I fully understand and share the concerns raised about the protection of journalistic sources so as to enable a free press. My office published some initial advice on this matter via our website on 4th September 2014. This publication sought to highlight and explain the law in relation to Part I Chapter 2 of RIPA and to importantly explain how complaints are dealt with when non-compliance is suspected. We highlighted that, as the law stands at the moment, communications data generated by communications companies are business records, but recognised that, when in the possession of the police and analysed such data can be used to quickly identify who has communicated with whom and inference can be drawn as to why those communications have taken place.

The communications data code of practice was drafted some eight years ago and, unlike the interception or the surveillance code which were recently updated, contains no advice on dealing with professions that handle privileged information, or the use of confidential help-lines which is problematical in itself as our role is primarily to inspect public authorities on their compliance with the Act and its code. The Government's Note on the European Court of Justice Judgment[41] outlines the Government's intention to amend the communications data code of practice, ensuring that where there may be concerns relating to professions that handle privileged information (for example, lawyers or journalists), public authorities give additional consideration to the level of intrusion. During the passage of the Data Retention and Investigatory Powers Act (DRIPA) there were several interventions during the debates about legal privilege and matters relating to journalists. The Minister James Brokenshire stated the Government will be amending the code of practice on the acquisition and disclosure of communications data later this year (see Hansard 15 July 2014: Column 816)[42] and I urge the Home Office to expedite matters to bring about early public consultation. There needs to be an informed discussion to bring about an agreement as what that advice will be. Any advice should take into consideration the case law relating to various rulings regarding freedom of expression when intertwined and balanced against, for example, the prevention or detection of crime or matters relating to national security.

Today I have written to all Chief Constables and directed them under Section 58(1) of RIPA to provide me with full details of all investigations that have used Part I Chapter 2 RIPA powers to acquire communications data to identify journalistic sources. My office will undertake a full inquiry into these matters and report our findings publicly so as to develop clarity in relation to the scope and compliance of this activity. *My office will also be contributing to the public consultation of the communications data code of practice which should, according to what was indicated in Parliament, start later this year. I would urge all those who feel strongly about this topic to also contribute to the consultation."*

The Rt Hon. Sir Paul Kennedy (interim Commissioner July – December 2014)

[41] www.gov.uk/government/uploads/system/uploads/attachment_data/file/331106/DRIPgovernmentNoteECJjudgment.pdf
[42] http://www.publications.parliament.uk/pa/cm201415/cmhansrd/cm140715/debtext/140715-0004.htm

Annex B

Chief Constable

6th October 2014

Dear Chief Constable,

IOCCO Inquiry into the use of RIPA powers to acquire communications data relating to the confidential sources of journalists

My role is to keep under review the acquisition of communications data by public authorities under Part I Chapter 2 of RIPA and report my findings to the Prime Minister on a half-yearly basis.

You will, I am sure, have seen the recent media reporting concerning the police acquiring communications data for the purpose of identifying journalistic sources. The media reporting to date has focused on Operations Alice (Metropolitan Police Service) and Solar (Kent Police) and has made several references about the appropriateness of the use of RIPA powers in relation to journalistic privilege.

My office published some advice on this matter via our website on 4th September 2014. This publication sought to highlight and explain the law in relation to Part I Chapter 2 of RIPA and to importantly explain how complaints are dealt with.

The communications data code of practice, unlike the interception code, contains no advice on dealing with professions that handle privileged information. However there is understandable public concern (which I share) about the necessity and proportionality and the potential intrusion caused by such access, not least due to the importance of protecting journalistic sources so as to ensure a free press. There is also case law relating to various rulings regarding freedom of expression when intertwined and balanced against, for example, the prevention or detection of crime.

The Government's Note on the European Court of Justice Judgment[43] outlines the Government's intention to amend the communications data code of practice, ensuring that where there may be concerns relating to professions that handle privileged information (for example, lawyers or journalists), public authorities give additional consideration to the level of intrusion. During the passage of the Data Retention and Investigatory Powers Act (DRIPA) there were several interventions during the debates about legal privilege and matters relating to journalists. The Minister James Brokenshire stated the Government will be amending the code of practice on the acquisition and disclosure of communications data later this year (see Hansard 15 July 2014: Column 816)[44].

[43] www.gov.uk/government/uploads/system/uploads/attachment_data/file/331106/DRIPgovernmentNoteECJudgment.pdf
[44] http://www.publications.parliament.uk/pa/cm201415/cmhansrd/cm140715/debtext/140715-0004.htm

I readily accept that there needs to be an informed discussion to bring about an agreement as to what the amendments to the code of practice might be. The purpose of the inquiry that I have launched today is to develop clarity in relation to the extent and compliance of this activity, to reassure the public in relation to the use of RIPA powers, and, to better inform any review of the legislation.

We expect applications for communications data under these circumstances will be exceptionally rare. The table overleaf contains a request for the number of investigations undertaken by your police force in the past 3 years that have involved determining if a member of a police force or other party have been in contact with a journalist or employee of a newspaper or television company related to news / documentaries, and, if Part I Chapter 2 RIPA powers were used, details of the communications data acquired, the person/s the data related to and the purpose of the acquisition.

You may consider this request to be part of your general duty under Section 58(1) of RIPA to *"disclose or provide to the Interception of Communications Commissioner all such documents and information as he may require for the purpose of enabling him to carry out his functions under Section 57 of the Act."*

I would be grateful if you could arrange for the Senior Responsible Officer (SRO) under Part I Chapter 2 of RIPA to provide the required information to my office by Monday 13th October 2014. I thank you in advance for your assistance with this inquiry.

If you have any queries regarding the content of this request or consider that there will be difficulties in meeting the deadline please do not hesitate to contact us.

Yours sincerely,

The Rt Hon. Sir Paul Kennedy
Interception of Communications Commissioner

cc Senior Responsible Officer (SRO) for Part I Chapter 2 of RIPA,
Single Point of Contact (SPoC) Manager

IOCCO Inquiry into the use of RIPA powers to acquire communications data relating to journalistic sources

Please complete the below request for information and return with the required documentation to info@iocco.gsi.gov.uk by Monday 13th October 2014.

Name of Public Authority:

Number of investigations which involve determining if a member of police force or other party have been in contact with a journalist or employee of a newspaper or television company related to news / documentaries in past 3 years.	

For each investigation above provide:

1. A brief outline of the investigation specifying the role of the journalist / employee.
2. Details of the crime / offences under investigation.
3. Details of any communications data that was acquired on the journalist / employee or the person suspected to be in contact with them. Please list the communications data acquired (type of data, date parameters, person data related to, and, purpose of acquiring the data).
4. Submit copies of any such communications data applications including the Designated Persons (DPs) considerations.
5. Submit copies of any legal advice that was sought / provided in relation to journalistic privilege / protecting journalistic sources.

Number of investigations in past 3 years where a PACE order has been applied for to require disclosure of journalistic material / the identity of a journalistic source.	

For each investigation above provide:

1. A brief outline of the investigation specifying the role of the journalist / employee.
2. Details of the crime / offences under investigation.
3. Details of the material sought.
4. Details as to whether the Judge granted / refused the order and the reasoning.

It is appreciated that it might not be a straightforward task to identify such investigations / communications data applications. Liaison with your Head of Crime Investigations, Professional Standards Department / Anti Corruption Unit and Senior Investigating Officers (SIOs) combined with targeted searches across force systems / communications data workflow systems might assist.

Annex C

Information excluded from the inquiry

1.1 There were circumstances when police forces had undertaken investigations where the journalist had been the victim of a crime and communications data was required to investigate that crime. They included malicious and nuisance communications such as death threats and threats of violence (not necessarily related to their role as a journalist). There were also instances where journalists had received anonymous information relating to threats and this had been brought to the attention of the police with a view to the police investigating or intervening.

1.2 Several police forces undertook liaison with us to determine whether certain activity and the subsequent investigation their force had undertaken was captured by our requirements for information. This included, for example, several instances of social messaging undertaken in the midst of a criminal trial by an unknown person – there was no indication that the person was a journalist; or the use of a website to publish information about the members of a police force relating to their private lives and allegations made against them.

1.3 The inquiry team concluded from the submissions made by the police forces that no court orders (for example section 9 schedule 1 PACE) were undertaken in order to acquire communications data to determine a journalist's source.

Investigations Undertaken by Metropolitan Police Service (MPS)

1.4 Due to the territorial spread of the MPS the majority of national news and media organisations have their headquarters and operational offices within its primary jurisdiction and, therefore, the fact that the MPS has initiated or been required to undertake such investigations is dictated by that geographical relationship.

1.5 The MPS are currently conducting several investigations which significantly impact on matters related to Article 10 of the Convention. These investigations have

been highlighted in the media and, in addition, Operations Elveden and Weeting were, due to their nature, subject of extensive comment in the Leveson Inquiry[45].

1.6 Prior to considering the communications data requests undertaken by the MPS it is important to explain the role of the Management and Standards Committee[46] (MSC). News Corporation established the MSC to take responsibility for all matters in relation to phone hacking at News of The World, payments to the police and all other related issues at News International. The MSC is autonomous from News Corporation and News International. It works to ensure full co-operation with all investigations into these issues, including the Leveson Inquiry, the police inquiries, civil proceedings and Parliamentary hearings. The MSC is authorised to conduct internal investigations to fulfil its responsibilities in relation to New International's papers: The Sun, The Times and The Sunday Times. It has power to direct News International staff to co-operate fully with all external and internal investigations, and to preserve, obtain and disclose appropriate documents.

1.7 We think it appropriate to highlight Operation Weeting which began on 26 January 2011 when News International disclosed, what the MPS has described as significant new information relating to allegations of phone hacking at the then News of the World (2005-2006). As a consequence of the investigations into the unlawful interception of voicemail messages very significant amounts of communications data were obtained by Operation Weeting relating directly to the role of journalists. The majority of this communications data was obtained by Operation Weeting <u>without</u> engaging powers within Chapter 2 of Part 1 of the Act. The explanation given by the senior investigating officer was as follows –

> *A line of investigation was to identify instances where those suspected of being involved in a conspiracy to intercept voicemail messages had either intercepted voicemail messages themselves, or had been party to the tasking and dissemination of information gleaned from other conspirators, who had themselves conducted the intercept.*

[45] See page 421 onwards – Volume 1 https://www.gov.uk/mwg-internal/de5fs23hu73ds/progress?id=CmDO9ma+y8&dl
[46] The role of the MSC is explained in the Leveson Inquiry report - see Part E, Chapter 5 Volume 1 https://www.gov.uk/mwg-internal/de5fs23hu73ds/progress?id=CmDO9ma+y8&dl

News UK were requested by the MPS to consider disclosing mobile telephone billing records in their possession[47] for those employees suspected of being part of that conspiracy. News UK located copy billing in their finance office archive.

Mobile telephone billing data was disclosed by News UK in hardcopy form and was not subject to any redactions prior to disclosure and included –

- *150,000 individual rows of mobile phone data (billing) for periods between December 2001 and July 2006 relating to 16 individual employees of News UK.*
- *The data was supplied in two disclosures in June 2012.*

1.8 The applications for communications data that had been submitted under the Act within Operation Weeting (and the sub-operations) were examined by the inquiry team and we are able to confirm that the emphasis of the investigation was / is not to identify journalistic sources. As such this investigation has been excluded from the inquiry. However, the fact that a significant amount of the data acquired relates to journalists inevitably raises concerns that the analysis of this data whilst in the possession of the police may subsequently be used to identify journalistic sources.

1.9 Another matter, reported in the media, concerns the disclosure of communications data in error within MPS Operation Elveden. During the course of the investigation very significant amounts of communications data were disclosed by Vodafone to the MPS in error. Matters relating to the circumstances of the error have been investigated and we have previously published information about it[48].

[47] A telephone company can make available to the customer 'copy bills' and 'unbilled usage'. Customers such as large companies will normally retain copies for accounting purposes. These records distinguish which of the telephones on the account have made specific communications i.e. outgoing calls and SMS & MMS messages together with the time, date and duration.
[48] See http://www.iocco-uk.info/docs/IOCCO%20Press%20Release%20re%20Vodafone%20Disclosure%20Error.pdf

Annex D

PROPOSED GUIDANCE FOR OFFICERS CONSIDERING A REQUEST FOR JOURNALIST COMMUNICATIONS DATA UNDER RIPA 2000

Anne Flanagan[49]

The issue of who today is a journalist in the era of social media where anyone can publish has been discussed by various commentators, including the author. As a result of having read such an article[50] by the author, the Interception of Communications Commissioner's Office inquiry team looking into use of communications data to identify journalistic sources, requested whether it would be possible to draft succinct guidance on this topic. This potentially was for use by police officers in considering requests for access to the communications data of persons who might be considered journalists. The guidance would need to provide workable criteria to enable officers making such decisions to balance the respective interests at stake, including freedom of expression.[51] One of the key concerns with such guidance was not to be unduly prescriptive as to which publications might fall under the heading of 'journalism' in light of the fact that many non-traditional forms of media are used to distribute communications of great public interest. Yet, not every public communication will carry the same freedom of expression weighting in the balancing with other interests. The guidance below attempts to provide a practical distillation of the criteria considered in the balancing under relevant jurisprudence to be used in the context of various media.

Proposed Guidance

Courts have found that journalists as 'watchdogs' for democratic societies are entitled under the right to freedom of expression to enhanced safeguards from unnecessary and disproportionate intrusions on their right and duty to convey ideas and information in the public interest, including the right to protect confidentiality of sources. They have also held that, with today's numerous online communication platforms, what comprises 'journalism' should not be unduly limited to traditional outlets. Not every form of expression, however, amounts to journalism. The following criteria may assist in deciding whether something is

[49] Professor of Law, Queen Mary University of London, Centre for Commercial Law Studies. I am grateful to my colleague Professor Ian Walden for his kind review and comments. The guidance, however, represents my views alone.
[50] See A. Flanagan, 'Defining 'journalism' in the age of evolving social media: a questionable legal EU test' *Int J Law Info Tech (Spring 2013) 21 (1): 1-30.*
[51] There may not be a statutory privilege for journalist communications, however, under the Human Rights Act 1998, e.g., public authorities have an obligation to act and make decisions in accordance with the European Convention on Human Rights to the greatest extent possible. Thus, the necessity for and the proportionality of a request for access in light of the circumstances would need to be considered in making the decision in balancing the qualified right to freedom of expression under Article 10 and the competing public interest.

journalism in considering whether a request under RIPA for a journalist's communications data should be made / approved. In addition, this provides guidance as to how this information should on balance be used in making this application/decision.

Journalism is the gathering, verification and dissemination of news and other information that the public needs in their daily lives and to participate as citizens. Whether those that engage in journalism are paid or work for traditional media organisations is irrelevant. Also irrelevant is the technology or format used.[52] What is key to distinguishing journalism or expression entitled to the enhanced safeguards from other kinds of communications is whether it meets two criteria: the content should meet a threshold public interest test; it should also be accurate and reliable under journalism standards.

The greater the public interest in publishing or receiving certain information or expression, the more likely that it will be subject to enhanced protection under the right to freedom of expression, even where it is uncertain that it comprises 'journalism' as such. What information or expression is in the public interest is not the same as whether it is interesting to the public. Public interest in information or expression instead relates to its need and value in the lives of people and their ability to participate in a democratic society. There is no set or finite list of information or expression that is in the public interest to publish or receive. If however there were a sliding scale of public interest, issues like the conduct of government (national and local) and matters concerning politics would likely be considered as having the greatest public interest. Information on topics like finance, health, religion, science, crime, national security, culture and the arts are also likely to have a high level of public interest. At the other end of the scale, mere 'tittle tattle', gossip and tawdry details about personal lives are likely to have a much lower level of public interest. So, if a publication addresses issues with a greater public interest factor like political speech, this should get greater weight in the balancing of interests as to whether an intrusion on the journalist's freedom of expression might be justified.

[52] Journalism often uses social media forms appropriate to the situation which may serve as helpful examples here. See, e.g. 'Peter Jukes is named best UK Reporter on Twitter and social media – full Press Gazette top 50 list', Press Gazette (8 April 2014), http://www.pressgazette.co.uk/peter-jukes-named-best-uk-reporter-twitter-and-social-media-full-press-gazette-top-50-list ; L. Oberst, 'Journalism and Social Media: 15 Examples Worth Learning From', Centre for Sustainable Journalism (26 Oct 2011), http://sustainablejournalism.org/socialmedia/journalism-social-media-examples.

Accuracy and reliability are hallmarks of journalism accorded enhanced protection.[53] To ensure accuracy and reliability, journalism requires accurate and reliable sources. Additionally, journalism should generally be transparent about its sources so that the reader can form an opinion as to its reliability and accuracy. It should also be transparent as to the distinction between what is conjecture, fact and comment.[54] Any significant inaccuracies should be corrected. Using the standard of accuracy and reliability, a publication comprising unsubstantiated rumours and accounts without reference to sources or attribution is not generally considered journalism. Therefore, whether a publication discloses how the facts were acquired and their context, including where it cannot disclose the source and why, can help to distinguish protected journalism from other communications.

A request for communications' data under RIPA that involves the detection or prevention of a crime is a legitimate interest that can justify a limitation on freedom of expression. However, the specific intrusion must also be necessary and proportionate under the circumstances in order not to infringe the right to freedom of expression subject to enhanced protection such as journalism. This requires further analysis. If the crime is unrelated to journalism even though a journalist is involved, no extraordinary consideration arises. For example, if a journalist has threatened to kill someone, obtaining communications data to ascertain information needed to prevent this from occurring would be essential. As no compelling public interest in journalism is involved here, heightened protections don't arise. If a journalist has witnessed a crime about which he writes, journalism is involved. The need for the information, the seriousness of the crime, possibilities that it could recur are all factors that would weigh on whether the intrusion is necessary. Consider, for example, the scenario where a journalist is merely one of several witnesses and the information to which any such communications data might lead, although convenient, is not needed either to prosecute or prevent a recurrence of the crime, even if serious. On balance, it might be considered an unnecessary intrusion on freedom of expression. This concern applies equally to use of a journalist's communications data to identify a confidential source of information. Its use could have a *chilling effect* on sources' willingness to provide important information and undermine the press' vital 'public watchdog' role and ability to provide accurate and reliable reporting. Here any countervailing public interest in access to the information must

[53] Financial Times v UK, ('Article 10 protects a journalist's right – and duty – to impart information on matters of public interest provided that he is acting in good faith in order to provide accurate and reliable information in accordance with the ethics of journalism').
[54] See The Editor's Code of Practice, Independent Press Standards Office, https://www.ipso.co.uk/assets/1/Code__A4_2014.pdf.

be compelling and balanced against the necessity for the intrusion. So, if alternative evidence exists for the information that might be obtained via a journalist's communications data, access to the data would be unnecessary. It might also be disproportionate depending on the scope of the data sought. Absent such compelling interest and exigent circumstances, recourse to the other sources of information should be sought.

Also absent such circumstances, in no case should communications data be sought or approved in order to obtain access to a journalist's confidential source and thereby bypass the more restrictive legal framework that exists for this under the Contempt of Court Act 1981, i.e. where disclosure is necessary in the interests of justice or national security or for the prevention of disorder or crime.

Annex E

Further review of law, policies, guidance and other matters influencing police investigations relating to leaks to the press, police corruption and misconduct in public office

1.1 Where an investigation relates to an allegation of criminal conduct by a member of a police force, that police force (or another public authority appointed to investigate the complaint) may use their powers under Chapter 2 of Part 1 of the Act to obtain communications data for the purpose of preventing and detecting the alleged or suspected crime where the investigating officer intends the matter to be subject of a criminal prosecution[55]. That means the police cannot use their powers within the Act to acquire communications data when the criminal threshold (i.e. the use of the statutory purpose at section 22(2)(b)) has not been met or the sole intention of obtaining evidence is merely to make an officer or member of their staff subject to an internal discipline hearing. So, should it be determined there are insufficient grounds to continue the criminal investigation or insufficient evidence to initiate a prosecution within a criminal court, it will, with immediate effect, no longer be appropriate for the police force to obtain communications data under the Act.

1.2 Misconduct in a public office is a common law offence which has existed for many years. As the Court of Appeal noted in the case of *Attorney General's Reference No.3 of 2003 [2004] EWCA Crim 868*, the circumstances in which the offence may be committed are broad and the conduct which may give rise to it is diverse. There are four essential elements of the offence, namely -

1. The suspect must be a public official acting as such;
2. He or she must have wilfully breached his/her public duties;
3. The breach must have been such a serious departure from acceptable standards as to constitute a criminal offence; and to such a degree as to amount to an abuse of the public's trust in the public official; and
4. There must have been no reasonable excuse or justification.

[55] See section 81(4) of the Act – concerning "criminal proceedings" and criminal prosecution

1.3 The third and fourth elements of the offence of misconduct in a public office are critical. Commissioner Hogan-Howe in his evidence to the Leveson Inquiry[56] observed that:

> *"I would never argue for every leak to be investigated. I think you can drive yourself barmy, I think, if we did that. It is where the consequences are serious or it might display a pattern of behaviour that we want to investigate. It's those things that are of concern to me, not … tittle-tattle … that will happen from time to time, but it is if it starts to damage our reputation in terms of the integrity of how we handle confidential information and sometimes secret information, which it is vital we have that – for the trust of our partners and of the public that we are able to maintain that sort of secrecy."*

1.4 There is a threshold and it is a high one. In particular, as the Court of Appeal recognised in the case of *AG's Reference No.3 of 2003*, to attract criminal sanctions, the misconduct in question would normally have to amount to an affront to the standing of the public office held and to fall so far below the standards accepted as to amount to an abuse of the public's trust in the office holder.

1.5 The Crown Prosecution Service (CPS) has published guidance in relation to the investigation and prosecution of cases where public servants have disclosed confidential information to a journalist. The CPS view potential prosecution cases involving journalists or journalist's sources sufficiently serious that all cases are, in the first instance, referred to their Special Crime Division (SCD). After consideration by SCD some cases may, by agreement, be handled at Area or Sector level by suitably qualified lawyers, or referred to Counter Terrorism Division if consideration is being given to charging an offence under one of the Official Secrets Acts.

1.6 The Independent Police Complaints Commission (IPCC) was established by the Police Reform Act 2002 and became operational in April 2004. It has therefore completed seven years as an operational body investigating incidents and complaints.

[56] See http://www.levesoninquiry.org.uk/wp-content/uploads/2012/03/Transcript-of-Morning-Hearing-20-March-2012.pdf pp63-64, lines 13-1, Commissioner Hogan-Howe

Its primary statutory purpose is to secure and maintain public confidence in the police complaints system in England and Wales. In addition to this statutory responsibility, the IPCC also has in its guardianship role, an obligation to measure, monitor and where necessary, seek to improve the current system.

1.7 The IPCC has published two reports concerning corruption in the police service within England and Wales. The report was ordered by the Home Secretary, under powers set out in the *Police Reform Act 2002*, in a statement to the House of Commons in July 2011. The statement followed allegations concerning corrupt relationships between the police and the media generated by the News of the world phone hacking story -

> *In July 2011 unprecedented levels of public concern were expressed regarding allegations of phone hacking by News of the World journalists. A number of developments including arrests by the Metropolitan Police Service (MPS), the discovery of emails held by lawyers used by News International and civil cases involving high profile individuals culminated in revelations that messages on Milly Dowler's mobile phone had been listened to and deleted during the time she was missing. This prompted an intense two week period of reporting of further matters, including allegations that unnamed police officers had received illegal payments in exchange for confidential information.*

1.8 In addition to the Home Secretary using her powers under section 11(2) of the Police Reform Act 2002 to request a report on the IPCC experience of investigating corruption in the police service, the Prime Minister and the Home Secretary also commissioned other inquiries which included -

- *A judge-led inquiry ("the Leveson inquiry"[57]) into the culture, practices and ethics of the press and the extent of unlawful or improper conduct within News International and other newspaper organisations;*
- *An inquiry by Her Majesty's Inspectorate of Constabulary (HMIC) into undue influence, inappropriate contractual arrangements and other abuses of power in police relationships with the media and other parties.*

[57] See http://webarchive.nationalarchives.gov.uk/20140122145147/http:/www.levesoninquiry.org.uk/ and the Executive Summary at https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/229039/0779.pdf

1.9 The HMIC report was also in two parts. The first, undertaken by HMIC, was to "*consider instances of undue influence, inappropriate contractual arrangements and other abuses of power in police relationships with the media and other parties*". The resulting report, Without Fear or Favour (HMIC 2011)[58] included the following observation [emphasis added] -

> *"We found that forces lack the capacity and capability to proactively identify any inappropriate relationships. Forces conveyed a sense of inevitability that resourcing complex investigations into media leaks rarely yields any positive results. Forces should explore options for identifying and monitoring emerging and inappropriate relationships with, and leaks to, the media.*
>
> *HMIC asked forces to complete a questionnaire detailing the total number of investigations conducted in relation to information disclosure since April 2006. HMIC analysis of the data supplied by forces shows that disclosure to the media is the only area of information disclosure which has not seen a significant increase. Over this period 302 (4%) of inappropriate information disclosures investigated by forces related to disclosures to the media. (58 investigations resulted in action being taken, and 63 are continuing.)*
>
> *Forces were also asked to provide data on the total number of investigations conducted in relation to inappropriate relationships with the media in the last five years. HMIC analysis of the data provided shows only 12 investigations were conducted (excluding information leaks). Of these, in one case the member of staff resigned; one investigation resulted in reprimand; one in a warning; one in management advice; one is ongoing; and seven concluded with no further action required.*
>
> *HMIC found a general understanding amongst staff at all levels that leaking information to the media about operational matters is unprofessional, unacceptable and a breach of standards.*
>
> *Although the data provided to HMIC shows that reported inappropriate information disclosure to the media is relatively rare, HMIC's survey work showed that 43% of respondents thought that disclosure of sensitive information to the media was 'a very' or 'fairly big' problem. This demonstrates that when such leaks do occur, the impact on the public's perception is significant.*

[58] See http://www.justiceinspectorates.gov.uk/hmic/media/a-review-of-police-relationships-20111213.pdf

All forces have some form of policy, procedure or guidance on dealing with the media: but these are of variable quality and currency. There is limited consistency between force policies, although many refer to the ACPO Communications Advisory Group guidance. Only three force policies provide clarity around managing and maintaining relationships between staff and the media, and even they do not seek to define the boundaries of appropriate relationships."

1.10 HMIC made several recommendations which included that [emphasis added]-

"Forces and authorities institute robust systems to ensure risks arising from relationships, information disclosure, gratuities, hospitality, contracting and secondary employment are identified, monitored and managed. They should ideally do so on the basis of national standards and expectations – there are no geographical variables when it comes to integrity and there should not be local differences in standards. This work on national standards should be encouraged by the Home Office and promoted by leaders in the Service locally."

1.11 The second report was produced by Dame Elizabeth Filkin at the request of the then Commissioner of the Metropolitan Police, Sir Paul Stephenson. This examined the *'ethical issues arising from the relationship between the police and the media'*.

1.12 The IPCC, citing the report by Dame Elizabeth Filkin, within their second report - 'Corruption in the police service in England and Wales: second report – based on IPCC's experiences from 2008 – 2011[59]', acknowledged [emphasis added]-

It [Filkin, 2011] concluded that the perception that MPS personnel leak to the media was prevalent and damaging. While Filkin found little hard evidence, she believed that improper disclosure to the media was occurring and, if left unregulated, would continue to harm the MPS and the public. Her report specifically defines three areas of concern with regard to MPS-media relations: the unauthorised disclosure of information; the relationships that allow this to happen; and the extent to which this area was regulated. The subsequent seven recommendations included the need for officers and staff to make a

[59] http://www.ipcc.gov.uk/sites/default/files/Documents/research_stats/Corruption_in_the_Police_Service_in_England_Wales_Report_2_May_2012.pdf

brief personal record of the information they provide to the media. Senior managers were recommended to create an atmosphere that deterred improper disclosure of information and to strongly pursue leaks via criminal or misconduct sanctions.

1.13 Filkin, when giving evidence to the Leveson Inquiry[60] noted,

"*.....investigations of leaks tend to be futile and resource-intensive*....."

1.14 The Association of Chief Police Officers (ACPO) has published a paper called the ACPO Police Integrity Model (2013)[61] which sets out a checklist for chief officers to consider when applying the model within their organisations which includes [emphasis added] -

- *Commit to zero tolerance approach to corruption and a graduated and proportionate approach to investigation and sanctions;*
- *Commit to the Independence Police Complaints Commission definition of corruption and the force anti-corruption strategy; and,*
- *Commit to internal and external communication of corruption outcomes.*

1.15 The College of Policing has published 'Guidance on relationships with the Media' (2013)[62] suggests that-

If you have a relationship with a specific journalist on a personal basis outside of your role as a police officer or member of police staff (such as a relative or close friend), details should be logged within your force in accordance with local policy and procedure.

1.16 Parliament is presently considering the Criminal Justice and Courts Bill[63] which creates a new criminal offence of police corruption. Clause 25 will make it an offence for a police officer to exercise the powers and privileges of a constable in a way which is corrupt or otherwise improper. It supplements the existing common law offence of

[60] http://www.levesoninquiry.org.uk/wp-content/uploads/2012/03/Transcript-of-Afternoon-Hearing-5-March-2012.pdf235 pp10-11, lines 22-8, Elizabeth Filkin
[61] See http://www.acpo.police.uk/documents/workforce/2013/201301-wfd-police-integrity-model.pdf
[62] See http://www.acpo.police.uk/documents/reports/2013/201305-cop-media-rels.pdf
[63] See http://services.parliament.uk/bills/2014-15/criminaljusticeandcourts.html page 68

misconduct in public office. On 6 March 2014, the Home Secretary made a statement to the House of Commons, setting out the findings of the Stephen Lawrence Independent Review, conducted by Mark Ellison QC –

> *"The current law on police corruption relies on the outdated common-law offence of misconduct in public office. It is untenable that we should be relying on such a legal basis to deal with serious issues of corruption in modern policing, so I shall table amendments to the Criminal Justice and Courts Bill to introduce a new offence of police corruption, supplementing the existing offence of misconduct in public office and focusing clearly on those who hold police powers."* [Hansard, 6 March 2014, Column 1065]

1.17 A statement by the Government concerning the Criminal Justice and Courts Bill explains –

> *While the overwhelming majority of police officers act honestly and with integrity, the Government believes that the small minority of officers who act in a way which falls short of these standards must be made subject to the full force of the criminal law. The British public have every right to expect police officers, as the guardians of the law and the Queen's Peace, to conduct themselves to a higher standard than other public servants.*
>
> *If police officers fail to conduct themselves to those high standards, it is right that we should seek to uphold that higher standard by means of the criminal law. We believe that the best way to do this is to create a new offence of police corruption, solely applicable to police officers, to sit alongside the existing, broader, common law offence. This will serve the dual purposes of punishing appropriately those who act corruptly and of deterring those who might consider such acts in the future.*