

Witness Name: Paddy McGuinness

Statement No.: 1

Date: 13 January 2016

THE UNDERCOVER POLICING INQUIRY

WITNESS STATEMENT OF PADDY MCGUINNESS

I, PADDY MCGUINNESS, will say as follows:

INTRODUCTION

1. I am authorised to make this statement on behalf of the Cabinet Office and do so in response to the Inquiry's Rule 9 Request dated 30 November 2015. I have read this Request and seek here to respond to it to the best of my ability.
2. I make this statement from my own knowledge and experience of working within Government, and in particular my experience of working in an environment which requires dealing with classified and highly sensitive material. Where matters are not within my own knowledge, I have relied on information and documentation made available to me and I have also drawn on the wider expertise of individuals from the Foreign and Commonwealth Office, Home Office, Ministry of Defence, Ministry of Justice, the Government Communications Headquarters, the Secret Intelligence Service, and the Security Service, (these last three I shall refer to collectively as "the Agencies").

3. I am currently engaged as a Deputy National Security Adviser in the National Security Secretariat at the Cabinet Office. I am responsible for intelligence, security and resilience and have undertaken this role since January 2014. I am specifically responsible for supporting the Prime Minister and National Security Adviser on counter terrorism; intelligence policy; the governance and resourcing of the Agencies; cyber security; and resilience and crisis management. I have extensive national security experience from service in the UK and overseas. I do not however hold any legal qualifications and in addressing the Inquiry's request it has been necessary to set out the application of the neither confirm nor deny ("NCND") principle with reference to previous Court and Tribunal judgments. I have done so with the assistance of legal advisers.
4. The National Security Secretariat provides advice to the Prime Minister on matters of national security. In doing so it works closely with various parts of the national security machinery of Government which most regularly apply the NCND principle. I am therefore using this experience to illustrate the application of the principle primarily with reference to the Agencies.
5. I wish to make clear at the outset that this statement does not directly address the use of the NCND principle by the police. Police forces, including the Metropolitan Police, are not part of any Government department or Agency. As far as the application of the principle by Government is concerned, this seeks to illustrate how it has been applied in practice. However, as will become clear, the application of the principle in individual cases is necessarily a matter to be considered by the department or Agency concerned on the basis of all the facts of any particular case.

WHAT IS NCND?

6. NCND is an acronym for 'Neither Confirm Nor Deny'. The NCND principle is a mechanism used to protect sensitive information and applies where secrecy is necessary in the public interest; and where this mechanism avoids the risks of damage that a confirmation or denial would create. As noted by the Investigatory

Powers Tribunal (IPT) in *Belhadj & Others v Security Service & Others* [2015] UKIPTrib 13_132-H at paragraph 21, NCND is not in itself a statutory rule. However, the principle of protecting sensitive information where necessary, is explicit in the statute governing the IPT, in particular section 69(6)(b) of the Regulation of Investigatory Powers Act 2000 and Rule 6(1) of the Investigatory Powers Tribunal Rules 2000.

7. It has also been reflected in the Official Secrets Act 1911 to 1989, the Data Protection Act 1988, and the Freedom of Information Act 2000, which contain exceptions for information concerning national security, as well as the legislation governing the Agencies, namely the Security Service Act 1989 and the Intelligence Services Act 1994.
8. By its very nature, the work of the Agencies provides the paradigm example of a context in which secrecy is required if the work is to be effective, and there is an obvious, and widely recognised, need to preserve that effectiveness. This requirement of secrecy has long been recognised by the Courts. Lord Griffiths stated in *Attorney General v Guardian Newspapers Ltd (No.2)* ("Spycatcher") [1990] 1 A.C. 109 at paragraph 269:

"The Security and Intelligence Services are necessary for our national security. They are, and must remain, secret services if they are to operate efficiently....."

9. It is also to be noted in that respect that the Security Service and Intelligence Services Acts place a duty on the heads of the Agencies (i.e. the Director General of the Security Service, the Chief of the Secret Intelligence Service and the Director of the Government Communications Headquarters) to ensure that no information is disclosed by the relevant Agency except so far as necessary for the proper discharge of its functions (see section 2(2)(a) of the 1989 Act and sections 2(2)(a) and 4(2)(a) of the 1994 Act – "the statutory provisions on disclosure of information").

10. There may be a variety of different reasons for needing to keep information relating to the work of the Agencies secret. For example, if a hostile individual or group were to become aware that they were the subject of interest by the Agencies, they could not only take steps to thwart any covert Agency investigation or operation; but also attempt to discover, and perhaps reveal publicly, the methods used by the Agencies, their capabilities and techniques, or the identities of the officers or agents involved. Compromise of any of this information would affect both the individual investigation or operation and potentially all others. It could also jeopardise the future willingness of agents or prospective agents to cooperate and put at personal risk the officers and agents concerned and others with whom they have had dealings. These sorts of concern are also likely to apply to undercover operations conducted by the police.

11. Successive governments have therefore taken decisions to neither confirm nor deny assertions, allegations or speculation in relation to the Agencies. This, means that, as a general rule, the Government will adopt a position of NCND when responding to questions about whether the Agencies are carrying out, or have carried out, an operation or investigation into a particular person or group; have a relationship with a particular person; hold particular information on a person; or have shared information about that person with any other agencies, whether within the UK or elsewhere. I understand that police forces in England and Wales also adopt a similar position, applying the NCND principle when responding to questions about operations, investigative techniques and methods, and in relation to information about individuals, be they officers, or informants, or suspects.

12. NCND is most often applied in the context of the work of the Agencies, However, the NCND principle is also applied by other parts of Government (and by police forces and other law enforcement bodies):

- a. These include the Ministry of Defence. They will adopt an NCND stance to avoid revealing information which might for example enable foreign States or hostile actors to thwart any military operation or to

discover the methods, capabilities and techniques used by the forces (particularly those branches that operate covertly), or the identities of the personnel involved. Compromise of such information could affect not only current, but potentially future, operations and could undermine both the effectiveness and deterrent effect of our armed forces.

- b. They also include the National Offender Management Agency (NOMS), an executive agency of the Ministry of Justice which has the responsibility for the running of prisons and the probation service in England and Wales. NOMS is able to authorise the use of Covert Human Intelligence Sources (CHIS) for the purpose of preventing or detecting crime or otherwise in the interests of public safety and will use NCND in relation to requests for information about the use of CHIS to protect these sources from harm and to ensure that the use of covert tactics is sustainable in the future.

THE INTRODUCTION AND DEVELOPMENT OF NCND

13. The term 'Neither Confirm Nor Deny' appears to have first entered the lexicon in the 1950's; although, as I shall explain below, this was not the first use of the underlying principle. In 1958, the Operations Coordinating Board, which was part of the US National Security Council, made the decision that it would neither confirm nor deny the presence or absence of nuclear weapons at any locations. This had the effect of creating uncertainty about the location of nuclear weapons which would reduce an adversary's military planning capability and reduce the chance of a successful attack. This is one of the first occasions on which such an approach was referred to specifically using the term, 'neither confirm nor deny'.

14. In February 1975, the media reported the leak of a document which purported to describe an alleged project called the Global Marine Explorer Project (often referred to as Glomar). This project is said to have involved the US Central Intelligence Agency (CIA) seeking to recover intelligence and military materials from a Soviet submarine which had sunk in the Pacific Ocean. A request was

made under United States legislation, which I understand is similar to the Freedom of Information Act in England and Wales, asking the CIA to confirm the existence of the project and to provide related records. The CIA refused to 'either confirm or deny' the existence of the project or provide any records, a position which was upheld by the US courts who agreed it was acceptable in the interests of national security. The courts agreed that to have either confirmed or denied the existence of the project or its outcome could have handed a significant advantage to the Soviet Union during a time of heightened diplomatic and political strain.

15. Since the Glomar incident the phrase has become widely adopted. However, the underlying rationale had already been recognised and accepted by courts in the UK at least as far back as the judgment of Pollock CB in *Attorney General v Briant* (1846) 15 M. & W. 169 (at paragraph 185) which recognised that in general the identities of informers should not be revealed:

"...the rule clearly established and acted on is this, that in a public prosecution a witness cannot be asked such questions as will disclose the informer, if he be a third person. This has been a settled rule for fifty years, and although it may seem hard in a particular case, private mischief must give way to public convenience..."

16. Thus, the principle of neither confirming nor denying allegations in order, in the public interest, to maintain the secrecy of information where necessary is one that has been recognised and upheld for many years. The NCND principle, and its basic nature and underpinning, has remained constant. Over the years, it has been applied in a variety of different situations.

THE APPROACH TO NCND AND ITS APPLICATION IN PRACTICE

17. In order to be effective the NCND response must be applied consistently, including when no activity has taken place and a denial could properly be made. If the Government denied a particular activity in one instance, the inference might

well be drawn that the absence of a denial in another amounted to confirmation of the alleged activity.

18. *In re Scappaticci* [2003] NIQB 56, Carswell LCJ explained the basis for the maintenance of NCND as follows:

"To state that a person is an agent would be likely to place him in immediate danger from terrorist organisations. To deny that he is an agent may in some cases endanger another person, who may be under suspicion from terrorists. Most significant, once the Government confirms in the case of one person that he is not an agent, a refusal to comment in the case of another person would then give rise to an immediate suspicion that the latter was in fact an agent, so possibly placing his life in grave danger.

...There is in my judgment substantial force in these propositions and they form powerful reasons for maintaining the strict NCND policy."

19. The Information Commissioner in his guidance (which can be found on his website at [www.ico.org.uk/media/for-organisations/documents/1166/when to refuse to confirm or deny section 1_foia.pdf](http://www.ico.org.uk/media/for-organisations/documents/1166/when_to_refuse_to_confirm_or_deny_section_1_foia.pdf)) relating to the application of NCND in relation to the Freedom of Information Act 2000 states as an overview:

"In certain circumstances, even confirming or denying that requested information is held can reveal information that falls under an exemption. A public authority may be able to use an exemption to refuse to confirm whether or not it holds information, if either confirming or denying would reveal exempt information in itself.

A neither confirm nor deny response is more likely to be needed for very specific requests than for more general or wide ranging requests.

It can be important to use a neither confirm nor deny response consistently, every time a certain type of information is requested, regardless of whether the information is actually held or not."

20. The Information Commissioner's guide also includes several illustrations of when an NCND response should be provided, for example:

"...a police force may hold information regarding particular properties they have under surveillance – it is likely that if a request were made for information about the surveillance of a certain property, this information would be exempt under section 30. A public authority could therefore refuse to confirm or deny whether it holds information about a property under surveillance.

Furthermore, this would apply even if information was requested about a property not under surveillance. If a police force only upheld its duty to confirm or deny where it was not keeping properties under surveillance, an applicant could reasonably assume that where the police force refused to confirm or deny, the property named in the request was under surveillance."

21. The guide provides further explanation of why consistency is important:

"A public authority receives a request for information about any prisoners who are under surveillance. The public authority judges that it would not be harmful to confirm that they hold information about this topic. However if they did not hold such information, then revealing this could be harmful as it would confirm to prisoners that they were not under surveillance. Therefore, whether or not information is held, the authority should refuse to confirm or deny.

If the public authority doesn't take this consistent approach then the occasions when it provides a neither confirm nor deny response may unintentionally imply whether or not information is held. For example,

Request 1: public authority confirms information is held;

Request 2: public authority confirms information is held;

Request 3: public authority states that it can neither confirm or deny that the information is held (the information is in fact not held);

Request 4: public authority confirms information is held.

Although the public authority hasn't actually denied that information is held for request 3, the different response could be interpreted as indicating that this is the case."

22. Where the Government is concerned, NCND is applied most frequently to prevent damage to national security and/or to ensure that government meets its responsibilities to protect the safety and lives of individuals (potentially engaging obligations under the European Convention on Human Rights ("ECHR") (notably, Articles 2 and 3)). NCND operates to protect against such damage both directly, for example in neither confirming nor denying agent status, and indirectly, for example by reducing the possibility that conclusions or inferences will be drawn through the non-consistent application of the principle.

23. The decision whether to maintain NCND will have regard to all the relevant facts and circumstances, and then weighing the public interests in play. As is obvious, it will often be the position that the public interest in protecting certain types of information (for example agent status, or sensitive operational techniques) will be very high indeed. That fact, coupled with the desirability of consistency of application of NCND, is likely to lead in practice to the situation in which cases of the Government not maintaining NCND in relation to well-

recognised types of information will be rare. That is not a reflection of a blanket or absolute, immutable policy. It is simply a function of the weight of public interest in maintaining necessary secrecy of the information in question, coupled with the desirability of maintaining consistency.

24. It will be for Government to make the initial decision about maintaining NCND. The judgements involved in assessing the needs of, for example, national security and the risks of damage attached to disclosure are paradigmatically for Government. As the Courts have consistently recognised (notably in the context of Public Interest Immunity (PII), but also in the context of proportionality analysis under the ECHR) the institutions of Government are best placed to make these judgements. As set out in the IPT case of *Steiner* (IPT/06/81/CH 2008, the Court in practice does defer to the judgement of the Government save in very narrow and extreme circumstances:

"The NCND response, if appropriate, is well established and lawful. Its legitimate and significant purpose and value has been discussed and ratified by the courts."

25. Courts adopt this approach on grounds of experience and institutional competence as only Government is likely to be able to see the whole picture affecting risks of damage, and sometimes on grounds of democratic accountability. It is the Government's responsibility to protect the lives and safety of the public and it is the Government which has specific responsibility to protect the safety of those who assist with fulfilling this obligation.

26. If the maintenance of NCND is challenged in a particular case, the resolution of that challenge will ultimately be a matter for a Court to determine, itself striking the requisite balance between the public interests in play in the case. The Government does not maintain, and has never maintained, that the NCND principle simply has to be asserted and then adhered to by Courts. As the Court of Appeal noted in *Mohammed v Secretary of State for the Home Department* [2014] EWCA Civ 559 at paragraph 20:

"...[whilst] there are circumstances in which the courts should respect [NCND]...it is not a legal principle. Indeed it is a departure from procedural norms relating to pleading and disclosure. It requires justification similar to the position in relation to public interest immunity (of which it is a form of subset)."

27. The NCND principle and its application by the Agencies was fully considered by the Information Tribunal in the Baker case (*Baker v Secretary of State for the Home Department* [2001] U.K.H.R.R. 1275).

- a. Norman Baker MP (as he was at the time), believed that the Security Service had a file on him, however his Subject Access Requests had been answered by a NCND response, supported by the national security exemption in section 28 of the Data Protection Act and the related Home Secretary certificate.
- b. In its decision of 1 October 2001 the Tribunal held that the blanket exemption given by the original certificate was wider than necessary to protect national security, as it relieved the Security Service of any obligation to give a considered answer to individual requests. However, although the Tribunal did not have to decide this particular point (which was not contested), in effect it endorsed the existence of and rationale for the NCND principle in its judgment.
- c. In its general observations, the Tribunal declared that this secrecy is necessary in order to safeguard national security, the importance of which in the contemporary world cannot be over-estimated. The Tribunal also confirmed that it was not in dispute that the Security Service was best-placed to decide whether or not and, if so, to what extent, an NCND response should be provided in an individual case.

28. Following the Information Tribunal's ruling, the Home Secretary signed a revised national security certificate. Following the issue of the revised certificate, Mr Baker brought fresh proceedings against the Security Service in the IPT (IPT/03/01). On 31 March 2004 the IPT gave its preliminary legal ruling, the net effect of which was as follows:

- a. Where personal data are processed, Article 8 of the ECHR will be engaged by an NCND response, and the interference will have to be justified on ECHR proportionality grounds.
- b. Where no personal data are processed, Article 8 will not be engaged, but an NCND response will have to be justified along *Wednesbury* reasonableness lines. (The *Wednesbury* test as to whether a decision is reasonable is a long-standing principle. It states that a decision should be considered unreasonable if no reasonable person acting reasonably could have made it.)

29. The IPT's final decision rejecting Mr Baker's complaint was given in September 2004. Although they gave no reasons, for present purposes the important point is that the IPT did not question the existence or rationale of the NCND principle. In fact, they upheld it in their preliminary decision of 31 March 2004 and endorsed it by their final decision. Their concern was rather to scrutinise the application of the NCND principle in practice by reference to the relevant test.

30. The Northern Irish case of *In re Scappaticci* (referred to above) provides another example.

- a. The claimant in that case alleged that his life was in danger because of media speculation that he had been an undercover agent working within the IRA as an informer for the security services. A Northern Ireland Office Minister declined his request to confirm that he was not an agent, and provided an NCND response. The court accepted that there was "a real and present danger" to his life. But that

notwithstanding, the Court refused to overturn the Minister's decision, and upheld the maintenance of NCND.

- b. Whilst the judgment in *Scappaticci* is expressed in the particular context of the threat posed by terrorist organisations, the rationale in relation to other circumstances where persons or organisations pose a threat of harm to agents or others providing information to the Agencies is the same. Neil Garnham QC (as he was then) advanced these arguments, with which I agree, in the Litvinenko Inquiry referring to the *Scappaticci* judgment,:

"...there will be occasions when confirming or denying information may be of vital and immediate importance to individuals interests, but because doing so would cause real and immediate damage to wider public interests, it would be wholly inappropriate, despite the disadvantage or risk of harm to the individual to do so. It follows that the policy of neither confirming nor denying must be applied consistently to be effective. That is so even where, in one particular case, the direct damage to wider public interests might appear, at first blush, to be slight."

- 31. As explained by the Security Service website, NCND is fundamentally important in the context of ensuring the safety of officers and agents:

"The breaking of promises of anonymity given to agents would also be likely to make existing and prospective agents unwilling to cooperate with the Service. Similarly, disclosing the identities of staff could put them at risk, compromise the operations on which they are or have been engaged, and limit how they could be deployed in the future."

- 32. The problems arising in the case of public reporting of allegedly sensitive information (whether by the press and/or by say an individual agent 'self-

declaring') may be acute. Perhaps the key point to note in such situations is that there is an important, substantive difference between the Government confirming or denying that a particular piece of information is true or not, and someone outside Government making the same assertion, however apparently well-informed that individual may appear to be. Only the Government can state with authority whether a matter previously kept secret is in fact true and claims, statements or purported disclosures made without official authorisation do not have any bearing on the application of the NCND principle. Thus the need to apply the NCND principle is likely to continue to exist even where an alleged agent may have publicly disclosed their own role or identity, but where there has been no official confirmation of the individual's claim.

33. The Inquiry has requested that I address so called 'exceptions' to the principle, their reasons and frequency. It is important to note that, once the principle is properly appreciated, it becomes evident that the 'exceptions' are in reality no more than the application of the principle itself. The decision whether or not to maintain NCND is a decision taken on the basis of a consideration and balancing of all the public interests in play in any particular set of circumstances. There are likely, as already noted, to be some kinds of information the protection of which will be heavily in the public interest – with the result that it would take something exceptional for the public interest to balance to come down in favour of disclosure. Nevertheless, decisions are made on a case by case basis in light of the particular range of circumstances that are in play.

34. The consequence is that cases in which NCND may not have been maintained are of limited value in predicting future decision making. This is because the new decision will be taken on the basis of all the circumstances of that particular case at that particular time.

35. In summary, NCND has been widely acknowledged and accepted as a mechanism for protecting sensitive information, by courts and tribunals, by Parliament and by successive UK Governments. Decisions about the application of NCND are properly in the first instance the responsibility of the Government as

the body with access to all the necessary information (including intelligence or other sensitive material) and with the democratic duty to protect the safety of its citizens. It is also important to keep in mind that even if no damage would be caused by the confirmation or denial of a specific piece of information, there is a legitimate public interest in the consistent application of the principle. This is particularly important where it is used to protect the safety of officers or agents.

36. Finally, it is worth remembering that the refusal of the Government either to confirm or deny an assertion or a suggestion about events under consideration indicates precisely nothing about the truth or otherwise of that assertion or suggestion.

I believe that the facts which I have stated in this statement are true.

Signed:

PADDY MCGUINNESS

Date:

13 January 2016

