

To 'Neither Confirm Nor Deny'

Assessing the Response and
its Impact on Access to Justice

About JUSTICE

Established in 1957 by a group of leading jurists, JUSTICE is an all-party law reform and human rights organisation working to strengthen the justice system – administrative, civil and criminal – in the United Kingdom. We are a membership organisation, composed largely of legal professionals, ranging from law students to the senior judiciary.

Our vision is of fair, accessible and efficient legal processes, in which the individual's rights are protected, and which reflect the country's international reputation for upholding and promoting the rule of law. To this end:

- We carry out research and analysis to generate, develop and evaluate ideas for law reform, drawing on the experience and insights of our members.
- We intervene in superior domestic and international courts, sharing our legal research, analysis and arguments to promote strong and effective judgments.
- We promote a better understanding of the fair administration of justice among political decision-makers and public servants.
- We bring people together to discuss critical issues relating to the justice system, and to provide a thoughtful legal framework to inform policy debate.

© JUSTICE 2017



JUSTICE

59 Carter Lane, London EC4V 5AQ

www.justice.org.uk

Contents

I.	Introduction	6
II.	Accessing Information	11
III.	Policy	18
IV.	Judicial Scrutiny	23
V.	The Investigatory Powers Tribunal	30
VI.	Accountability	35
VII.	Conclusion	40
VIII.	Recommendations	41
IX.	Acknowledgements	43

I. Introduction

1. The “neither confirm nor deny” (NCND) response is used by public authorities in a variety of contexts to avoid disclosing sensitive information. It may, for example be used by a government spokesperson in response to a question from the media, or in response to an access to information request.¹ The potential unfairness of the response is most acute in litigation.
2. This report focusses on the use of NCND within the framework of national security, surveillance and law enforcement, and builds upon previous JUSTICE reports on access to justice. *Secret Evidence*² looked at the use of closed material in courts, the right to a fair hearing and the core principles of the British justice system; *Freedom from Suspicion: Surveillance Reform for a Digital Age*³ considered the balance between surveillance and privacy, critiqued the Regulation of Investigatory Powers Act (RIPA) 2000 and made suggestions for reform; and *Freedom from Suspicion: Building a Surveillance Framework for a Digital Age*⁴ reflected upon the lack of transparency and accountability of decisions authorising surveillance.
3. The seminal case of *In re Scappaticci* shone a spotlight on the use of NCND.⁵ The applicant sought judicial review of a decision by the Minister of State at the Northern Ireland Office to neither confirm nor deny allegations that he was an undercover agent. He had denied the allegations publicly to no avail and his life had been threatened numerous times as he was suspected by the IRA of being an informer. The applicant argued that the Government owed him a duty under article 2 of the European Convention on Human Rights (the right to life) to confirm that he was not an agent. The applicant was not successful because, in Lord Chief Justice Carswell’s judgment:

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 [sic], 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.*⁶

4. The Court held that a departure from the NCND policy in this case would “endanger the lives of agents on other occasions” and have an impact on operational activity and intelligence-gathering.⁷
5. This explanation offers one of the clearest justifications for NCND and this report acknowledges that there are instances where public authorities can legitimately rely upon the NCND response. For instance, NCND may be suitable where there are ongoing undercover operations, or in certain situations where sensitive information has been relayed to government through an intelligence-sharing arrangement.⁸
6. Reliance on NCND has been criticised across various jurisdictions, particularly in the US⁹ where it is called the “Glomar response” in reference to judicial recognition of “neither confirm nor deny” in the case of *Phillippi v CIA*.¹⁰ Wherever NCND has been invoked, it has raised serious questions about access to justice.¹¹
7. The response restricts the amount of information available to litigants and therefore places barriers on parties being able to properly plead their case.¹² Despite stating otherwise, public authorities have often used NCND in a blanket fashion without properly assessing the risk of disclosure. Oxford Pro Bono Publico (OPBP) has pointed out the propensity of agencies across various jurisdictions to use NCND responses inappropriately in the pursuit of consistency. It has been used, for instance, in relation to:

*[R]equests for information about completely implausible government activities or operations, that could easily have been denied without harming national security. Similarly, the agencies have issued NCND responses to requests for information relating to programs which are already generally known about More problematic still is the use of NCND by agencies to conceal illegal or embarrassing conduct ...*¹³

¹ For an examination of the various contexts where a “neither confirm nor deny” response has been used, see the comparative research prepared by Oxford Pro Bono Publico, an organisation based at the University of Oxford’s Faculty of Law, conducted at the request of JUSTICE. Its research is presented as Annex I to this report. (Oxford Pro Bono Publico, “Neither Confirm Nor Deny”: Insights from Comparative Law, Policy Bodies, and Academia”, (February 2016)). We refer to this as ‘Annex I’. OPBP conducted further research based on specific questions posed by JUSTICE. These are also annexed and referred to as ‘Annex II’ (Oxford Pro Bono Publico, ‘Appendix: OPBP Further Research on ‘Neither Confirm Nor Deny’ (October 2017)). Please find the annexes online at <https://justice.org.uk/our-work/areas-of-work/criminal-justice-system/counter-terrorism-security/neither-confirm-deny-ncnd-response/>

² JUSTICE, *Secret Evidence* (June 2009), available online at <https://justice.org.uk/secret-evidence/>

³ JUSTICE, *Freedom from Suspicion: Surveillance Reform for a Digital Age* (October 2011), available online at <https://justice.org.uk/freedom-suspicion/>

⁴ JUSTICE, *Freedom from Suspicion: Building a Surveillance Framework for a Digital Age* (October 2015), available online at <https://justice.org.uk/building-a-surveillance-law-fit-for-purpose-new-justice-publication/>

⁵ [2003] NIQB 56.

⁶ *Ibid*, at para 15.

⁷ *Ibid*, at para 20.

⁸ However, note the recent joined appeal of *Belhaj & Another v Straw & Others and Rahmatullah (No 1) v Ministry of Defence & Another* [2017] UKSC 3 where the Supreme Court found that allegations of UK involvement in breaches of human rights by foreign governments were justiciable. See also Privacy International, ‘Human Rights Implications of Intelligence Sharing’ (September 2017), available online at <https://cryptome.org/2017/09/human-rights-spiid-pi.pdf>

⁹ Annex I, p. 5.

¹⁰ *Phillippi I*, 546 F. 2d. ‘Glomar’ refers to the Glomar Explorer vessel which sought to recover intelligence and materials from a sunken Soviet submarine in the 1970s. See Annex I, pp. 23-27 for a detailed discussion of the ‘Glomar response’, the background to its creation and how the response works.

¹¹ Annex I.

¹² For an example of the restrictions in the UK context, see Civil Procedure Rule 16.5 and *McGartland v Secretary of State for the Home Department* [2015] EWCA Civ 686.

¹³ Annex I, p. 12.

8. The use of NCND in this way weakens public trust in agencies and public authorities. Most crucially, it also risks undermining basic individual rights and the rule of law.¹⁴
9. In the UK civil courts, Lord Justice Maurice Kay has described NCND as a subset of Public Interest Immunity (PII).¹⁵ Under PII¹⁶ public authorities can obtain a certificate to refrain from disclosing certain material where it is deemed to be detrimental to the public interest. It can be used in civil or criminal proceedings. Similarly, the NCND response is a mechanism to protect sensitive information in the public interest.
10. However, the clear distinction between PII and NCND is that the trial judge and, where appropriate, special counsel are able to consider the material argued to fall under a PII claim, to assist in the judicial decision of whether the material should be disclosed or not.¹⁷ With an NCND response, the very existence of the material is in question and the court may have extremely limited information upon which to make an assessment, or be reliant on governmental assurances. This makes scrutiny of an NCND claim particularly problematic for the courts and tribunals where it is raised.
11. The restriction on disclosure of sensitive information is also referred to in the Freedom of Information Act 2000 (FOIA) and the Data Protection Act 1998 (DPA).¹⁸ Although these constitute important areas for consideration, this report focusses primarily on the operation of NCND in the civil courts and the Investigatory Powers Tribunal (IPT).¹⁹
12. In our view, the civil courts and the IPT have generally been too accepting of public authorities' decisions to use an NCND response. As JUSTICE highlighted in its 2011 report, *Freedom from Suspicion*:

*... it is somewhat disturbing that the courts have been so willing to accommodate NCND even at the cost of considerable damage to the principles of open justice and procedural fairness and ultimately their own integrity.*²⁰
13. We acknowledge that, in some cases, invocation of NCND has been subjected to judicial scrutiny, for example, in Sir Christopher Pitchford's recent, thorough review of NCND

¹⁴ *Ibid.*, p. 6 and 12.

¹⁵ Lord Justice Maurice Kay in *Mohamed Ahmed Mohamed, CF v Secretary of State for the Home Department* [2014] EWHC Civ 559, at para 20; NPCC, 'Submissions on behalf of the NPCC on the Principle of Neither Confirm nor Deny', *Undercover Policing Inquiry*, 21st January 2016, at para 7 available online at <https://www.ucpi.org.uk/wp-content/uploads/2016/03/160121-submissions-on-the-NCND-principle-NPCC.pdf>

¹⁶ PII is a rule of evidence established through case law and was first applied in the case of *Duncan v Cammell Laird* [1942] AC 624.

¹⁷ See Crim PR 22.3; *R v Jackson* [2000] Crim LR 377; *R v Austin* [2014] 1 WLR 1045.

¹⁸ The Information Commissioner's Office has provided guidance to public authorities on FOIA and personal data. See ICO, 'When to refuse to confirm or deny information is held: Freedom of Information Act', 18 December 2013, available online at https://ico.org.uk/media/for-organisations/documents/1166/when_to_refuse_to_confirm_or_deny_section_1_foia.pdf; and ICO, 'Neither confirm nor deny in relation to personal data: Freedom of Information Act, Environmental Information Regulations', 22 May 2013, available online at https://ico.org.uk/media/for-organisations/documents/1206/neither_confirm_nor_deny_in_relation_to_personal_data_and_regulation_foi_eir.pdf

¹⁹ For a discussion of NCND in relation to FOIA and personal data, see Annex I, pp. 16-23.

²⁰ See note 3, *Freedom from Suspicion* (2011), at para 393.

in the Undercover Policing Inquiry.²¹ However, open judgments do not consistently subject the response to rigorous or structured examination. We believe that such a serious departure from procedural norms requires robust interrogation in every case. In Chapter 4 we suggest some solutions to this. The absence of consistently rigorous scrutiny of the NCND response to date reflects the judiciary's reticence in challenging the executive on issues deemed to relate to national security.²² Judicial deference to the executive is understandable given the executive's access to classified information and the perception that the courts are ill-equipped to make determinations when it comes to national security.²³ OPBP considers that this is further exacerbated by mosaic theory, which posits "that the disclosure of even seemingly innocuous information can threaten national security, by enabling adversaries to piece together a picture of national security practices."²⁴ Bearing in mind this context, the courts have a difficult job navigating the balance between open justice, natural justice and the need to serve national security interests.²⁵

14. In this report, JUSTICE examines the possibilities for the civil courts and the IPT to scrutinise the State party to litigation when NCND is used and ensure that complainants can hold public authorities to account in cases that rely on sensitive material. Consideration of appropriate standards that can balance competing public interests is timely considering the increased powers granted to judges in national security cases as a result of the

²¹ See Undercover Policing Inquiry, 'Restriction Orders: Legal Principles and Approach Ruling' (3 May 2016), at paras 113-162, available online at <https://www.ucpi.org.uk/wp-content/uploads/2016/05/160503-ruling-legal-approach-to-restriction-orders.pdf>

²² In the case of *Secretary of State for the Home Department v Rehman* [2003] 1 AC 153, Lord Hoffmann at para 50 highlighted that "decisions as to whether something is or is not in the interests of national security are not a matter for judicial decision. They are entrusted to the executive." However, he states at [54] that this does not surrender the whole decision to the executive and the judiciary has an important role to play within the prism of the separation of powers. Lord Hoffmann's speech was referred to at length by Lord Neuberger in *R (Lord Carlile of Berriew QC) v Secretary of State for the Home Department* [2014] UKSC 60, at paras 22-26. He notes at para 30 the Crown's prerogative to conduct foreign relations and take measures in the interest of national security, but where there is interference with Convention rights, "there can be no absolute constitutional bar to any inquiry which is both relevant and necessary to enable the court to adjudicate."

²³ The European Parliament's report 'National Security and secret evidence in legislation and before the courts: exploring the challenges' (September 2014), p. 9, available online at [www.europarl.europa.eu/RegData/etudes/STUD/2014/509991/IPOL_STU\(2014\)509991_EN.pdf](http://www.europarl.europa.eu/RegData/etudes/STUD/2014/509991/IPOL_STU(2014)509991_EN.pdf) states: "Claims of secrecy obstruct judicial scrutiny, and judicial authorities too often have to trust the quality and lawfulness of the information provided by the intelligence services and the legitimacy of state secrets claims." With respect to the US, Wessler considers some of these assumptions to deference and argues that the courts nevertheless have an important role to play in cases that concern national security, see N. F. Wessler, '[We] Can Neither Confirm Nor Deny the Existence or Nonexistence of Records Responsive to your Request', 85 *NYU Law Review* 1381, at paras 1398-1409.

²⁴ Annex I, at p. 10. The 'mosaic' theory is explicitly referred to in guidance produced by the Information Commissioner's Office. See for example ICO, 'International relations, defence, national security or public safety (regulation 12(5)(a)): Environmental Information Regulations', 11 June 2012, at paras 42-43, (available online at https://ico.org.uk/media/for-organisations/documents/1633/eir_international_relations_defence_national_security_public_safety.pdf) where the Commissioner states that he bears in mind the harm that may arise from a disclosure when assessing the arguments presented by a public authority.

²⁵ See Lord Neuberger's observations in *Al Rawi and Ors v The Security Services* [2011] UKSC 34, at para 74; and *Bank Mellat v HM Treasury (No. 1)* [2013] UKSC 38, at para 52.

Investigatory Powers Act 2016²⁶ and the increasing normalisation of closed material procedures following the Justice and Security Act 2013.²⁷

15. The report makes 23 recommendations for reform, across **five themes**:
- a. Accessing information – including that the Investigatory Powers Tribunal be given explicit and broader powers to **order** disclosure by the State;
 - b. Policy - in particular, a clear Government policy on the use of NCND analysed under the framework of the **proportionality test**;
 - c. Judicial scrutiny – including consistent application of a “**balance of interests**” test to NCND responses, and a presumption in favour of **open hearings** in the IPT;
 - d. Rules and procedures of the IPT –including the use of **cost orders** in exceptional circumstances and measures to improve procedures;
 - e. Accountability – improved **oversight**, an **appeals** mechanism and greater **expertise** on the IPT.

²⁶ The Investigatory Powers Act 2016 received Royal Assent on the 29th November 2016 and, at the time of writing, is not yet fully in force.

²⁷ See section 6. This is discussed in more detail below. See also Eva Nanopoulos, ‘European Human Rights Law and the Normalisation of the ‘Closed Material Procedure’: Limit or Source?’, *Modern Law Review*, Vol. 78(6) (2015), pp. 913-994 which argues that European human rights law has not been a constraint on the expanded use of CMPs and has, instead, legitimised the practice and facilitated its further use.

II. Accessing Information

16. At its root, the NCND response creates barriers to access to justice because it limits the disclosure of information²⁸ and the State party’s pleadings, therefore having a negative impact upon a complainant’s ability to challenge alleged unlawful activity. The difficulties are exacerbated where the courts decline to consider information available in the public domain as being “officially confirmed”. In the case of *Baker v Secretary of State for the Home Department*,²⁹ the Information Tribunal stated that “official confirmation” is an “admitted exception” to the policy of giving an NCND response.³⁰
17. The issues relating to lack of disclosure and “official confirmation” are discussed in this section.

Disclosure

18. Disclosure of information is of central concern when a non-State party is faced with a “neither confirm nor deny” response. As Lord Kerr stated in his dissent in *Tariq*, the “withholding of information from a claimant which is then deployed to defeat his claim is, in my opinion, a breach of his fundamental common law right to a fair trial.”³¹ The cases discussed below relating to undercover policing, social justice and environmental activists offer the most egregious examples of utilising NCND to frustrate a claim by creating barriers to disclosure. The Undercover Policing Inquiry, which was opened on the 28th July 2015 following a series of high-profile allegations in the media of misconduct by covert human intelligence sources (CHIS) against political and social justice campaigners,³² is currently considering concerns surrounding disclosure.
19. Many of the victims and alleged victims of unlawful activity by undercover police officers and informants have described repeated encounters with the NCND response when seeking disclosure of information related to their case. Mills explains:

²⁸ The case of *Kennedy v The Charity Commission* [2014] UKSC 20 concerned the Freedom of Information Act 2000 and whether the Charity Commission had an absolute exemption from disclosing reports based on inquiries looking into an appeal founded by George Galloway MP. Among other issues, the Supreme Court considered whether article 10 ECHR (the right to freedom of expression) entails a right of access to information. In his leading judgment, Lord Mance found that article 10 did not impose a positive duty of disclosure on public authorities (para 94). Lord Wilson reached an alternative view in his dissent and stated at para 188 that “this court should now in my view confidently conclude that a right to require an unwilling public authority to disclose information can arise under article 10.”

²⁹ [2001] UKHRR 1275, at paras 33-34.

³⁰ N.B. Lord Justice Pitchford’s comments in the Undercover Policing Inquiry, see note 21, at para 127: “To my mind the circumstances and context in which disclosure is made may properly be described not as exceptions to a policy but the application of the policy.”

³¹ *Home Office v Tariq* [2011] UKSC 35, at para 108. Lord Kerr was referring to closed material procedures when making this point, but the principle espoused is applicable in the context of NCND.

³² For further explanation of the background to the inquiry, see ‘Undercover Policing Inquiry: Chairman’s Opening Remarks’ (28 July 2015), available online at <https://www.ucpi.org.uk/wp-content/uploads/2015/07/Opening-Remarks.pdf> This inquiry is now being led by Mr Justice Mitting, see ‘New panel member appointed Undercover Policing Inquiry’ (31 May 2017), available online at <https://www.gov.uk/government/news/new-panel-member-appointed-to-undercover-policing-inquiry>.

*'Neither Confirm Nor Deny' was the routine police response to their queries. That the police were prepared to go to considerable lengths to maintain this response became clear once the activists presented evidence produced by their own research to the police. It included dropping a prosecution case rather than reveal the presence of an undercover officer ...*³³

- 20.** Philippa Kaufmann QC noted in her submission to the Undercover Policing Inquiry that miscarriages of justice arose “precisely because the police failed to discharge their legal obligations to disclose their involvement in circumstances leading to the prosecutions.”³⁴ She criticised the police for failing to keep adequate documentation of undercover operations, leading to a situation where victims would not know they are victims unless they knew who the undercover officers were. In these circumstances, the victims would have to rely on the undercover officers disclosing their own identity to get to the truth – an “absurd proposition”.³⁵
- 21.** In relation to the identity of undercover officers alleged to have had relationships with activists, Helen Steel explained that the police did not use NCND during their interview with one of the activists and, in fact, confirmed that one of the individuals was a serving police officer. The Metropolitan Police only started using NCND once the *DIL* case was taken to court.³⁶
- 22.** These experiences demonstrate inappropriate recourse to NCND by public bodies, and insufficient assessments of the risks (if any) posed by disclosing information to those affected by allegedly unlawful activity. Excessive secrecy threatens access to justice, impedes the claimant’s ability to receive a fair trial and undermines the principle of open justice.³⁷ We agree with Dr Hadjmatheou that public authorities must, at every stage, undertake assessments on the risks to disclosing information and on a case-by-case basis.³⁸ This is particularly important in undercover policing operations where there appears to be a paucity of record-keeping³⁹ and insufficient attention given to whether disclosure genuinely undermines ongoing undercover operations. An interviewee relaying their experience of the undercover policing scandal said:

*[The police] gave us the standard ‘we can neither confirm nor deny’ the information that you’ve asked for. We then asked for an internal review and they completely ignored it. They didn’t even respond to that at all which is why we went for the Information Tribunal.*⁴⁰

- 23.** Taking note of these experiences, we welcome the comments made by Lord Justice Pitchford when setting out the legal principles and process of the Undercover Policing Inquiry:

*I accept the invitation by the police services and the Home Office to treat with due respect the risk assessments made by those who are expert in policing and the risks attendant on the exposure of identities and police operations. However, this acceptance does not mean that I shall accept every expression of opinion offered to me, particularly when the opinion is offered at the level of generality.*⁴¹

- 24.** Risk assessments and internal reviews are a necessary mechanism to enable the State to make appropriate use of the NCND policy and afford the courts proper scrutiny of its application. Instead of a process where NCND is accepted with little justification, with internal assessment the question can be properly asked as to whether answering an inquiry would harm a legitimate public interest on a case-by-case basis. Recently, the Chairman of the Undercover Policing Inquiry issued a direction to the Metropolitan Police Service (MPS) and, among other requirements, the MPS were directed to provide open and closed versions of risk assessments in respect of the real and cover names of individual undercover officers.⁴² This order offers a welcome example of recourse to risk assessments and should be replicated in other circumstances where there are concerns over the disclosure of sensitive information.
- 25.** Based on these risk assessments, the State party should present detailed justifications for the NCND response to the courts. The State party must recognise that NCND is not appropriate in every circumstance and must not be applied in a blanket fashion. Lord Justice Pitchford has observed that while an exception to the NCND policy “may have the impact of weakening its effect, it does not follow that making the exception will cause significant damage to the public interest.”⁴³ This approach accords with the decision in *Baker*⁴⁴ where the Information Tribunal found that the Secretary of State had issued an overly broad certificate exempting the Security Service from complying with an application under section 7 DPA – a provision that entitles the individual to be told that their personal data has been processed, by whom, why it is being processed and the source of the data.

³³ Helen Mills, ‘The undercover policing of political protest’, *Centre for Crime and Justice Studies* (21 October 2017), p. 5, available online at <https://www.crimeandjustice.org.uk/sites/crimeandjustice.org.uk/files/Undercover%20policing%20October.pdf>.

³⁴ Undercover Policing Inquiry, ‘Preliminary Hearing on the Legal Principles that Apply to the Application for Restriction Orders under Section 19 of the Inquiries Act 2005’, (23 March 2016), submissions by Philippa Kaufmann QC, p. 3, available online at <https://www.ucpi.org.uk/wp-content/uploads/2016/03/160323-transcript-of-hearing-on-23-March-2016-1.pdf>.

³⁵ *Ibid*, pp. 7-8.

³⁶ *Ibid*, submissions on behalf of the McLibel Support Campaign made by Helen Steel, pp. 146-152.

³⁷ See Lord Dyson’s comments in *Al Rawi v The Security Service* [2011] UKSC 34, at para 11: “The open justice principle is not a mere procedural rule. It is a fundamental common law principle.”

³⁸ Dr Katerina Hadjmatheou, ‘Neither Confirm Nor Deny: Secrecy and Disclosure in Undercover Policing’ (forthcoming) Dec. 2017, *Criminal Justice Ethics* Vol. 36(3).

³⁹ See note 34, submissions by Philippa Kaufmann QC, p. 7.

⁴⁰ See note 33, p. 4.

⁴¹ See note 21, ‘Restriction Orders: Legal Principles and Approach Ruling’, at para 161.

⁴² Undercover Policing Inquiry, ‘Order Pursuant to the Ruling of 2 May 2017 Granting an Extension of Time for Service of Anonymity Applications by the Metropolitan Police Service in Respect of the Special Demonstration Squad’, available online at <https://www.ucpi.org.uk/wp-content/uploads/2017/05/20170518-order-SDS-anonymity-applications.pdf>.

⁴³ See note 21, ‘Restriction Orders: Legal Principles and Approach Ruling’, at para 149.

⁴⁴ See note 29.

The Tribunal found that the Secretary of State applied the NCND policy more widely than was necessary to protect national security, and that the blanket exemption would relieve the Service of “any obligation to give a considered answer to individual requests.”⁴⁵ In our view, the Government should explicitly state in a coherent policy that NCND must be justified each time it is used (this is discussed in further detail below). It should be clear to public authorities that blanket refusals to disclose information are detrimental to the public interest and the interests of the non-State party.

- 26.** The issue of disclosure is also ever-present in the context of the IPT: the tribunal that hears cases concerning surveillance, interception of communications and investigatory powers. Our consultees pointed to instances of the State party giving an NCND response but then making late disclosure as a case progressed. For example, disclosures were made in the *Belhadj* case⁴⁶ that impacted on *Liberty/Privacy (No.1)*⁴⁷ and were later considered in *Liberty/Privacy (No. 2)*.⁴⁸ This suggests that greater disclosure of information in open proceedings is possible. Reflexive or routine resort to NCND by State parties at the outset, followed by eventual late disclosure, results in unfairness to the applicant(s).
- 27.** The reluctance of authorities to disclose is compounded by the fact that, although the IPT has the power to demand disclosure is filed with the tribunal in closed proceedings under section 68(6) RIPA, the IPT only requests that State parties disclose information to the other parties - it cannot order that they do so. In its 2016 report, the Tribunal notes that it has “received full and frank disclosure of relevant, often sensitive, material from those bodies of whom requests have been made” due to the “strength of the procedures” protecting sensitive information and the “confidence this inspires.”⁴⁹
- 28.** While it may be the case that the Tribunal’s requests are complied with in the majority of cases, we consider that there should be a presumption in favour of open disclosure, as this would ensure that accountability remains the priority for the IPT and all parties to the litigation. Further, we suggest that there would be more robust protection of the public interest if the Tribunal had a power to order disclosure in all circumstances where it considers that such an order is in the interests of justice, including to non-State parties. Such a power should be included in the IPT Rules (discussed below).

⁴⁵ *Ibid*, at para 113. The Information Tribunal’s decision is also discussed in the Pitchford Inquiry at paras 125-127.

⁴⁶ *Belhadj and others v Security Service and others* [2015] IPT/13/132/9H.

⁴⁷ [2014] IPT/13/92/CH.

⁴⁸ [2015] IPT/13/77/H.

⁴⁹ Investigatory Powers Tribunal, ‘Report of the Investigatory Powers Tribunal: 2011-2015’ (2016), at para 2.27, available online at http://ipt-uk.com/docs/IPT_Report_2011_15.pdf

Official Confirmation of Information

- 29.** The issue of “official confirmation” was raised in *DIL v Commissioner of Police of the Metropolis*.⁵⁰ The claimants – all of whom were environmental activists or social justice campaigners – sought damages arising out of long-term and intimate sexual relationships with alleged undercover police officers.⁵¹ The Defence relied on the “well established policy that the police will neither confirm nor deny ... whether a particular person is either an informer or an undercover officer.”⁵² Mr Justice Bean considered the application of the NCND policy following the claimant’s contention that the defendant was not entitled to rely on NCND to avoid pleading a full defence in accordance with rule 16.5(1) of the Civil Procedure Rules (CPR).⁵³
- 30.** In response to both the general allegations that undercover officers carried out unlawful activity and the claimants’ specific allegations⁵⁴ the defendant relied on NCND. The Metropolitan Police Commissioner argued that the policy exists “to protect undercover officers and to uphold the effectiveness of operations and the prevention and detection of crime.”⁵⁵ However, Mr Justice Bean held that there was “no legitimate public interest” in the Commissioner maintaining NCND in response to general allegations that undercover officers engaged in long-term, intimate relationships with activists.⁵⁶
- 31.** With regard to the specific allegations made by the claimants against the four alleged undercover officers, Mr Justice Bean noted that all the individuals had been publicly named by the media.⁵⁷ It was held that NCND could not be relied upon in two of the cases due to the fact that one of the individuals had been publicly named as an undercover officer by the Commissioner and the other had self-disclosed and been publicly named by the IPCC as a Metropolitan Police Officer. However, the identities of the other two individuals were not found to have been “officially confirmed” as neither individual had self-disclosed or been publicly named by an official,⁵⁸ thus revealing the judiciary’s caution when considering sensitive information.
- 32.** The *McGartland* case provides another example of the judiciary’s caution when accepting or rejecting information as being “officially confirmed”. The claimant alleged that he was an agent of the police and/or Security Services in Northern Ireland and claimed that the

⁵⁰ [2014] EWHC 2184 (QB).

⁵¹ Other claimants who alleged similar conduct brought claims through the *AKJ* litigation, see *AKJ v Commissioner of Police for the Metropolis* [2013] EWHC 32 (QB), and *AKJ v Commissioner of Police for the Metropolis* [2013] EWCA Civ 1342.

⁵² See note 50, at para 2.

⁵³ *Ibid*, at para 4. CPR 16.5(1) sets out that a defendant must state which of the allegations in the particulars of claim he denies; which he cannot admit or deny, but requires the claimant to prove; and which allegation he admits.

⁵⁴ The specific allegations were made by five individuals who alleged relationships with undercover officers. The claims are set out at paras 10-14 of the judgment.

⁵⁵ *Ibid*, at para 18.

⁵⁶ *Ibid*, at para 41.

⁵⁷ *Ibid*, at para 44.

⁵⁸ *Ibid*, at paras 45-47.

State had failed to protect him once his cover had been compromised. In response to his claims, the Secretary of State relied on NCND and submitted an application for a closed material procedure (CMP) under section 6 of the Justice and Security Act 2013,⁵⁹ which was accepted by Mr Justice Mitting in the High Court. The claimant appealed the decision and submitted that the judge should have considered the NCND issue first as it was “necessary for the purpose of determining whether the condition in section 6(5) was met, namely that it was ‘in the interests of the fair and effective administration of justice in the proceedings to make a declaration’.”⁶⁰ The claimants argued that the NCND policy served no useful purpose in this case because McGartland’s identity as a former police informant and security service agent had been both ‘officially confirmed’ and had been self-disclosed.⁶¹

- 33.** In the Court of Appeal, the claimants provided a body of material comprising official references to McGartland’s former role as a police informant. This included statements from Northumbria Police, a letter from the Home Secretary, and recitals to an agreement between McGartland, the Chief Constable of Northumbria Police, the Northumbria Police Authority, the Royal Ulster Constabulary and the Security Service recording that McGartland had provided valuable information to the security services.⁶² Lord Justice Richards found that this constituted “ample official confirmation of Mr McGartland’s role as a police informer, but in my judgment none of it amounts to official confirmation that he was an agent of the Security Service”.⁶³
- 34.** Lord Justice Richards reached this conclusion based on the case as pleaded and the material provided. He accepted that the Security Service was involved in McGartland’s resettlement but held that such information “falls short of official confirmation of the position.”⁶⁴
- 35.** These cases demonstrate the difficulties in compelling public authorities to disclose material and the judiciary’s reticence in accepting statements and documents from officials as “officially confirmed,” given the concern that accepting information as “confirmed” would undermine ongoing undercover operations.
- 36.** The ongoing Undercover Policing Inquiry is likely to address some of the barriers to disclosure. Lord Justice Pitchford’s statement on disclosure has, for example, set out a clear set of conditions “when considering whether to make an order restricting disclosure of *any relevant particular piece of information* on public interest grounds ...:

1. identify the public interest in non-disclosure;

- 2. assess the risk and level of harm to the public interest that would follow disclosure of that information;*
- 3. identify the public interest in disclosure;*
- 4. assess the risk and level of harm to the public interest that would follow non-disclosure of that information.*
- 5. make in respect of that information a fact sensitive assessment of that position at which the public interest balance should rest.”*⁶⁵

37. Further, the proposed “Hillsborough Law”⁶⁶ will help to improve the accountability of public authorities if passed by Parliament. Nevertheless, the cases considered in this section indicate that the judiciary may show undue deference to arguments offered by public authorities that disclosure would endanger national security.

38. Whilst disclosing genuinely sensitive information can pose a significant risk to national security and, in some circumstances, undermine the work of Covert Human Intelligence Sources (CHIS),⁶⁷ it is in the interests of open justice that the decision to use an NCND response not be taken lightly. We believe that the lack of a clear policy setting out how NCND should operate and how it should apply has undermined the judiciary’s ability to challenge public authorities when they rely on the response.

⁵⁹ CMPs are discussed in more detail below.

⁶⁰ See note 12, *McGartland*, at para 31.

⁶¹ *Ibid.*, at para 39.

⁶² *Ibid.*, at para 42.

⁶³ *Ibid.*, at para 43.

⁶⁴ *Ibid.*

⁶⁵ See note 21, ‘Restriction Orders: Legal Principles and Approach Ruling’, at para 152.

⁶⁶ Public Authority (Accountability) Bill. The Bill places a duty on public authorities and officials to act in the “public interest” with “transparency, candour and frankness”, and a duty to “assist court proceedings, official inquiries and investigations”. See ‘The Hillsborough Law’, available online at <https://www.thehillsboroughlaw.com/>

⁶⁷ JUSTICE’s report *Freedom from Suspicion* (2011) at para 306 recommended that complex operations involving undercover officers “be subject to authorisation by warrant issued by a Surveillance Commissioner or Circuit Judge.” The recommendation was made again in our follow-up report *Freedom from Suspicion* (2015) at para 30. In line with our previous reports, we reiterate our belief that CHIS is in need of substantial reform.

III. Policy

- 39.** In part, the barriers to access to justice have developed due to the absence of a clear and coherent policy on when NCND can be raised. A published, consolidated government policy would have the advantage of reinforcing the rule of law by enhancing transparency; providing government officials with a clear framework to follow when making a decision on whether to disclose sensitive information; and emboldening the courts to scrutinise the NCND response against the benchmark of the policy. The lack of an accessible policy has engendered a culture of secrecy and eroded faith in public authorities who have utilised NCND with insufficient regard to whether disclosure of information poses a genuine risk to national security or operational activity.⁶⁸
- 40.** The main justifications given by the State for use of NCND are only known from insufficiently detailed reports or have been revealed through witness statements as a consequence of litigation.
- 41.** One such witness statement was provided by Paddy McGuinness, the Deputy National Security Adviser in the National Security Secretariat at Cabinet Office, to the Undercover Policing Inquiry looking at the past conduct of undercover policing operations.
- 42.** Although McGuinness' expertise lay with intelligence matters, the Agencies (the Security Service, the Secret Intelligence Service and GCHQ) and other national security expertise, his witness statement noted the applicability of NCND to the policing context and outlined how the NCND policy works in practice. The statement explains that whilst NCND is not enshrined in statute, it forms part of the protection of sensitive information which is "explicit" in the statute governing the IPT,⁶⁹ the IPT's rules, and has been reflected in various other statutes.⁷⁰ McGuinness also notes that the need to preserve the effectiveness of the work of the Agencies has been recognised in case law and that there is a duty on the heads of the Agencies to ensure that disclosure is confined to that which is necessary for the proper discharge of its functions.⁷¹
- 43.** In relation to the work of the Agencies, the witness statement justifies the NCND policy by reference to mosaic theory and the threat that disclosure could pose to covert investigations or operations.⁷² It also provides a background to the response;⁷³ sets out that it must be applied "consistently";⁷⁴ explains that the Government makes the initial decision

whether to maintain NCND based on the public interest;⁷⁵ notes that the Government and its institutions are "best placed" to make judgements about the risks of disclosure, but emphasises that the Government does not maintain that the courts should simply adhere to the Government's judgement.⁷⁶ Throughout, McGuinness makes reference to key cases and concludes that 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."⁷⁷ Notably, Lord Justice Pitchford explicitly referenced McGuinness' witness statement in his ruling on the Undercover Policing Inquiry and stated that NCND "does not ... have a life of its own,"⁷⁸ thereby rejecting the proposition that NCND must be applied "consistently".

- 44.** Another such occasion where a governmental official explicitly referenced the NCND policy was through the witness statement of Charles Farr, the Director General of the Office for Security and Counterterrorism. It was provided to support the Government's position in a case brought by NGOs alleging the unlawfulness of certain assumed activities of the Agencies as a result of the Snowden leaks. Similar to McGuinness' statement, Farr justifies the NCND response by reference to the protection of national security, mosaic theory and the need to maintain secrecy in relation to ongoing operations and interception techniques.⁷⁹ He also provides a rationale for the general policy that there will be an NCND response to requests about monitoring individuals:

Take, for example, the case where an individual alleges that he is being targeted by the Intelligence Services, when he is in fact of no interest to them. It might not cause any damage to national security in that particular case for the Intelligence Services to deny any targeting of that individual. However, such a denial has the real potential to cause indirect national security damage. This is because there may be a future case where a similar allegation is made by a person or organisation who is of genuine interest to the Intelligence Services. Damage would of course be caused by confirming the allegation, but damage would also be caused by a 'no comment' response as it would be interpreted as an inferred admission, given the previous denial.⁸⁰

- 45.** In practice, this position amounts to a blanket policy that undermines the principle of open justice. It presents the Agencies with the opportunity to use an NCND response to avoid revealing the true extent of a surveillance regime. It has also created a situation where information about alleged conduct in relation to investigatory powers has only been

⁶⁸ See note 38, Hadjimatheou, 'Neither Confirm Nor Deny: Secrecy and Disclosure in Undercover Policing'.

⁶⁹ This Act is the Regulation of Investigatory Powers Act 2000.

⁷⁰ See Paddy McGuinness's Witness Statement to the Undercover Policing Inquiry, at paras 5-7 <https://www.ucpi.org.uk/wp-content/uploads/2016/01/NCND-PDF-unsigned-witness-statement.pdf>

⁷¹ *Ibid*, at paras 8-9.

⁷² *Ibid*, at para 10.

⁷³ *Ibid*, at paras 13-16.

⁷⁴ *Ibid*, at paras 17-21.

⁷⁵ *Ibid*, at paras 22-24.

⁷⁶ *Ibid*, at paras 24-26.

⁷⁷ *Ibid*, at para 33.

⁷⁸ See note 21, 'Restriction Orders: Legal Principles and Approach Ruling', at para 116.

⁷⁹ Charles Farr's Witness Statement in *Liberty/Privacy (No. 1)* [2014] IPT/13/92/CH, at paras 42-48, available online at <https://www.liberty-human-rights.org.uk/sites/default/files/Witness%20statement%20of%20Charles%20Farr%20on%20behal%20of%20the%20Intelligence%20Services%2016th%20May%202014.pdf>

⁸⁰ *Ibid*, at paras 44-45.

exposed following high-profile leaks – most clearly demonstrated through the Snowden revelations. At the very least this is “unsatisfactory”⁸¹ and, as discussed above, the operation of NCND restricts access to information and disclosure.

46. Nevertheless, McGuinness’ statement and the six paragraphs dedicated to NCND in Farr’s statement constitute the clearest explanations from officials of the Government’s position. This is an inappropriate approach to accountability that requires rectification if there is to be trust in a public authorities’ motivations for surveilling an individual or intercepting information. We believe that it is insufficient to rely on witness statements to justify a policy that impedes access to justice and that Lord Justice Maurice Kay described as a “departure from procedural norms”.⁸² We agree with numerous submissions to the former Independent Reviewer of Terrorism Legislation that a clear NCND policy would provide much-needed accountability.⁸³ Concerns about the operation of NCND would be partly alleviated if there were an accessible policy or, as the Reviewer’s 2015 report explains, if public authorities “at least summarise[d] the legal advice or assumptions on which they are operating”.⁸⁴ NCND may be used in a broad range of scenarios – from general public discourse to specific questions about surveillance programmes⁸⁵ – and a coherent NCND policy would be a sensible and simple step toward improving transparency.

47. When formulating its policy, the Government should utilise the language of “proportionality” which has been applied in key cases and judgments to consider how NCND may interfere with Convention rights or other fundamental rights recognised at common law.⁸⁶ As Lord Reed explained in *Bank Mellat (No. 2)*, proportionality is a generally accepted principle of EU law and has also been applied in the context of the ECHR.⁸⁷ In both circumstances, the “intensity” of its application depends on the context and the rights at stake.⁸⁸

48. The criteria for assessing proportionality, as developed by domestic case law under the Human Rights Act 1998, are as follows:⁸⁹

1. *Whether the objective of the measure is sufficiently important to justify the limitation of a protected right,*
2. *Whether the measure is rationally connected to the objective,*
3. *Whether a less intrusive measure could have been used without unacceptably compromising the achievement of the objective, and*
4. *Whether, balancing the severity of the measure's effects on the rights of the persons to whom it applies against the importance of the objective, to the extent that the measure will contribute to its achievement, the former outweighs the latter.*

49. By using the proportionality test as a framework, the Government can develop a consistent and rights-focussed policy to consider the public interest in disclosure versus the public interest in maintaining confidentiality. This would make clear to public authorities that they cannot apply NCND as a mantra, but only as a last resort.

50. The policy should include example scenarios to indicate where an NCND response may or may not be required and how NCND policy should be generally applied, such as has been issued by the Information Commissioner’s Office in relation to freedom of information requests and access to personal data.⁹⁰ It could set out a public authorities’ broad approach and then the specific balance of interests considerations where a complainant requests certain information relating to, for example, an undercover agent, foreign intelligence, directed surveillance, interception of communications data, or informants.

51. A section relating to undercover agents could explain, through the prism of the proportionality test, for example, that:

- The NCND response would broadly constitute a sufficiently important objective because it protects the undercover agent from any risks to their life or harm they may suffer as a consequence of their identity being revealed; it maintains the integrity of ongoing operational activity; and in some circumstances protects the identities of other undercover agents.
- The NCND response would be rationally connected to the objective of protecting the undercover agent and may, in fact, engage the undercover agent’s right to life under article 2 ECHR.
- When determining whether a less intrusive measure could be used than NCND, the public authority should look at its risk assessments (as discussed above) to inform its judgement about the impact of disclosure.
- If it concludes that a less intrusive measure than NCND could not be used, the public authority would then have to consider the balance of interests. At the general level the policy could say that an individual’s rights (for example, the right to

⁸¹ This point was made in a number of submissions to the Independent Reviewer of Terrorism Legislation’s review, see David Anderson QC, Independent Reviewer of Terrorism Legislation, *A Question of Trust: Report of the Investigatory Powers Review*, (June 2015) at para 12.5, available online at <https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2015/06/IPR-Report-Print-Version.pdf>

⁸² See note 15, Lord Justice Maurice Kay LJ in *Mohamed Ahmed Mohamed, CF*, at para 20.

⁸³ This is also reflected in research by OPBP in Annex I which, at p. 79, urges agencies to “adopt and publish clearer guidelines for how NCND is used – and that those guidelines should be more consistently applied.”

⁸⁴ See note 81, David Anderson QC, *A Question of Trust*, at para 12.17.

⁸⁵ Annex I, pp. 4-9.

⁸⁶ See for example *R (Lord Carlile of Berriew QC) v Secretary of State for the Home Department* [2014] UKSC 60.

⁸⁷ See Annex 2 for a discussion of proportionality, legitimate aim and the “necessary in a democratic society” criterion.

⁸⁸ [2013] UKSC 38, at paras 68-76. However, proportionality under the Convention is linked to the margin of appreciation: an understanding that a national court may be better placed than the Strasbourg court to understand the appropriate balance to be struck. This approach was reaffirmed by Lord Sumption in *R (Lord Carlile of Berriew QC) v Secretary of State for the Home Department* [2014] UKSC 60, at paras 19-21. For a detailed discussion of proportionality and how it is applied in different contexts, see Lord Reed’s comments in *R (Lumsdon & Ors) v Legal Services Board* [2015] UKSC 41.

⁸⁹ *Ibid*, at para 74.

⁹⁰ See note 18, ICO guidance.

privacy) will not normally outweigh the safety of the undercover agent and the need to avoid compromising ongoing operational activity.

52. Though this example reinforces the availability of the NCND response, it does not mean that it should be applied without diligence. A policy, together with the internal risk assessment we recommend in chapter II would ensure rigorous engagement with the issues raised by NCND and the policy must be explicit in acknowledging that it admits exceptions. So there would, for example, be a different balancing exercise if an individual requests information about an undercover agent where the undercover agent is (a) no longer a member of the security services, (b) has been accused of unlawful activity that took place decades ago, (c) faces no credible threats to their life if their identity is uncovered, (d) the life of another is at risk through the non-disclosure of the undercover agent's identity, and/or (e) revealing their identity would have a negligible impact on ongoing operations.
53. Taking another example, requests for information about surveillance would warrant a different set of considerations than the identity of an undercover agent. Relying on an NCND response to allegations of mass surveillance may serve the objective of protecting national security interests and ongoing operational activity, however it is debatable whether it is sufficiently important to interfere with the right to privacy.⁹¹
54. Within the policy, the government should set out its view of the legal basis for the NCND response. The IPT noted in *Belhadj* that “NCND is not in itself a statutory rule” but section 69(6)(b) RIPA 2000 and Tribunal Rule 6(1) require the IPT to give respect to the NCND principle.⁹² Therefore, the NCND response within the IPT has a clear foundation, however there is room for more clarity in other contexts and jurisdictions. As discussed above, McGuinness' witness statement made reference to statutes which “contain exceptions for information concerning national security, as well as the legislation governing the Agencies”, as well as a common law duty to requirement to maintain secrecy to preserve the effectiveness of the Agencies' work.⁹³ However, we believe that the government should offer a more comprehensive explanation of the sources that support the use of the NCND response.
55. We also consider that a public authority should give written reasons and justification for refusing access to an official document and this requirement should form part of the NCND policy. This would bring the policy in line with Art. 5 of the Council of Europe's Convention 205 on Access to Official Documents (which is not yet in force).⁹⁴

⁹¹ Indeed, one of our consultees pointed out that there have been examples of the IPT deciding that insufficient information was made public prior to proceedings to make a surveillance regime human rights compliant; for example, the sharing of information in *Liberty/Privacy (No. 1)* [2014] IPT/13/92/CH and the judgment in *Privacy International v Secretary of State for Foreign & Commonwealth Affairs & Ors* [2016] IPT/15/110/CH which said that secrecy over a particular power or tactic was unacceptable.

⁹² See note 46, *Belhadj v Security Service*, at para 21. The IPT's rules are discussed in more detail below.

⁹³ See note 70, McGuinness's Witness Statement, at paras 6-9.

⁹⁴ <https://rm.coe.int/1680084826> See also Annex 2 and Article 8 of the EU Charter of Fundamental Rights, which applies in the context of EU law (2000/C 364/01).

IV. Judicial Scrutiny

NCND in the Courts

56. Whilst it is important to protect sensitive information in the public interest, as cases like *Scappaticci* recognised, the presumption should be that NCND is a principle to be departed from “where the Tribunal is satisfied that there is a serious issue to be determined.”⁹⁵ The courts must be more willing to challenge the State party when they use NCND. As Lord Justice Maurice Kay warned, the courts must be vigilant when considering an NCND response, for:

*'... 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). It is not simply a matter of a governmental party to litigation hoisting the NCND flag and the court automatically saluting it. Where statute does not delineate the boundaries of open justice, it is for the court to do so.'*⁹⁶

57. This statement on the court's need to uphold the principle of open justice in the context of NCND is welcome. However, its application in practice is less clear, especially as a standard governing the NCND response in civil cases is lacking⁹⁷ and there has been increasing reliance on closed proceedings.
58. The public interest immunity (PII) principle offers an example of the courts considering the balance between competing public interests – known as the “*Wiley balance*”. As Lord Templeman explained in *ex parte Wiley*:

*Public interest immunity is a ground for refusing to disclose a document which is relevant and material to the determination of issues involved in civil or criminal proceedings. A claim to public interest immunity can only be justified if the public interest in preserving the confidentiality of the documents outweighs the public interest in securing justice.*⁹⁸

⁹⁵ See note 3, *Freedom from Suspicion* (2011), at [400]. A similar position was taken by the Bingham Centre for the Rule of Law. They submitted that “it is important to treat NCND as a starting point only, a defeasible principle that can be set aside where it becomes apparent to the IPT that it is necessary for the complainant to receive disclosure of material in order to effectively present his or her case.” (Bingham Centre for the Rule of Law, ‘The Investigatory Powers Review by the Independent Reviewer of Terrorism Legislation: Submission by the Bingham Centre for the Rule of Law’ (November 2014), at para 52, available online at https://www.biicl.org/documents/399_bingham_centre_submission_to_investigatory_powers_review_final_2014-11-19.pdf?showdocument=1)

⁹⁶ See note 15, *Mohamed Ahmed Mohamed, CF*, at para 20.

⁹⁷ In the criminal case of *Guardian News and Media Ltd v R & Erol Incedal* [2016] EWCA Crim 11, Thomas LCJ stated at para 49 that it is for the party seeking to curtail the principle of open justice “to make a very clear case” that it is “strictly necessary”. From our research, we found that, in general, NCND seems to be more rigorously tested in criminal proceedings than civil proceedings.

⁹⁸ *R v Chief Constable of the West Midlands Police, ex p. Wiley* [1995] 1 AC 274, at para 280.

59. However, the *Wiley* balance does not apply where there are closed material proceedings (CMPs).⁹⁹ The lack of a *Wiley* balance when considering a CMP application means that:

*'... whole swathes of information are not disclosable in these contexts even where the impact on national security would be relatively slight or remote but the interests of justice in disclosure are overwhelming. The result is that the majority of the evidence in a case, and often if not usually the entirety of the Government's factual case, remains undisclosed and is considered in closed ...'*¹⁰⁰

60. JUSTICE is concerned that the framework that governs disclosure in civil proceedings – through CMPs and NCND – empowers secret justice and restricts the complainant's ability to challenge the State party. A PII process may rely on NCND; however, even in the absence of any reliance on PII, the NCND response itself should always be subject to an established balance of interests test (akin to the *Wiley* balance).¹⁰¹ While some balance of interests undoubtedly takes place where NCND is invoked, as with the lack of a Governmental policy to its application, we submit that the assessment of the response by the courts is insufficiently robust. Judges should ensure they always apply an established framework, similar to the *Wiley* balance, to avoid being unduly deferential to national security arguments.

61. Given that, as described by Lord Justice Maurice Kay, NCND is a “subset” of PII, it should follow that the *Wiley* balance or a *Wiley* balance-type standard should apply whenever a public authority relies on the NCND response. The courts should be rigorous when assessing competing public interests to ensure that public authorities are not withholding disclosure for limited or insufficiently articulated reasons.

62. Where NCND is relied upon, the courts should use the opportunity to review the NCND response in detail and demand specific reasons from the State party, rather than boilerplate justifications,¹⁰² in line with the public policy we recommend above. Applying the *Wiley* balance, or a similar test, in each instance where NCND is raised would encourage the courts to avoid being overly deferential to national security arguments that have the potential to impact an individual's Convention rights or fundamental rights under the common law.

Closed Material Procedures

63. A closed material procedure requires the court to sit in private as well as excluding a particular party and their legal representative in order to protect sensitive information in

the interests of national security.¹⁰³ The 2011 Supreme Court case of *Al Rawi v The Security Service* provided the impetus for Part II of the Justice and Security Act 2013, which extended closed material procedures (CMPs) to all civil proceedings.¹⁰⁴ The respondents sought damages for the alleged involvement of the UK authorities in their detention, abuse of their human rights and their rendition by foreign authorities. The Government argued that the interests of justice would be better served by disclosing the relevant sensitive material through a CMP and would be preferable to a PII process.¹⁰⁵

64. When rejecting the Government's argument, Lord Dyson explained that open justice is a fundamental common law principle¹⁰⁶ and that “trials are conducted on the basis of the principle of natural justice”.¹⁰⁷ He concluded that it was not for the courts to extend such a controversial procedure without statutory authority.¹⁰⁸ Consequently, the Justice and Security Act (the Act) provided for CMPs to be available in civil proceedings.

65. To establish a closed hearing, the Secretary of State or any party to proceedings must make an application to the court for a declaration under section 6 of the Act. Under the same section, the court may make a declaration for a closed hearing “of its own motion.” Before making a section 6 declaration, the court must be satisfied that the Secretary of State has “considered whether to make, or advise another person to make, a claim for public interest immunity in relation to the material on which the application is based.”¹⁰⁹ Following that, two conditions must be met. Firstly, the court must ensure that sensitive information that concerns national security is not disclosed during proceedings.¹¹⁰ Secondly, that “it is in the interests of the fair and effective administration of justice in the proceedings to make a declaration.”¹¹¹

66. Throughout the proceedings the court should exercise its discretion when granting a section 6 application.¹¹² Section 14(2) of the Act provides that the framework for CMPs be subject to Article 6 ECHR.

⁹⁹ Discussed below.

¹⁰⁰ Tom Hickman, ‘Turning out the lights? The Justice and Security Act 2013’ (11 June 2013), UK Const. L. Blog, available online at <https://ukconstitutionallaw.org/2013/06/11/tom-hickman-turning-out-the-lights-the-justice-and-security-act-2013/>

¹⁰¹ Philippa Kaufmann QC submitted in *McGarland* that reliance on NCND requires justification similar to that used in PII. See note 12, *McGarland*, at para 38.

¹⁰² Annex I, at p. 13.

¹⁰³ CPR, Rule 82.6; see, for instance, the High Court's ruling that allegations over the role of former Foreign Secretary Jack Straw, former senior intelligence officer Sir Mark Allen, MI5 and MI6 in the extraordinary rendition of Libyan dissident Abdel Hakim Belhaj and his wife Fatima Bouchar should be held in closed proceedings. *Belhaj & Another v Straw & Others* [2017] EWHC 1861 (QB). It should be noted that a closed hearing is distinct from a private hearing. A private hearing excludes the public but allows the parties and their legal representatives to attend.

¹⁰⁴ See Joint Committee on Human Rights, ‘The Justice and Security Green Paper’ (4 April 2012), Twenty-fourth Report of Session 2010-2012, HL Paper 286, HC 1777, chapter 3, available online at <https://publications.parliament.uk/pa/jt201012/jtselect/jtrights/286/286.pdf>

¹⁰⁵ See note 25, *Al Rawi*, at paras 23-24.

¹⁰⁶ *Ibid*, at para 11.

¹⁰⁷ *Ibid*, at para 12.

¹⁰⁸ *Ibid*, at paras 47 and 69.

¹⁰⁹ Section 6(7).

¹¹⁰ Section 6(4) Justice and Security Act 2013.

¹¹¹ *Ibid*, section 6(5).

¹¹² Section 6(3); see also Mr Justice Popplewell's comments in *Belhaj & Another v Straw & Others* [2017] EWHC 1861 (QB), at para 19.

- 67.** Where a CMP takes place, the interests of a party may be represented by a Special Advocate¹¹³ – a barrister with security clearance. Communication between a Special Advocate and their client is heavily restricted due to the sensitivity of the material connected to the proceedings.¹¹⁴ The Special Advocate cannot communicate with the specially represented person or that person’s lawyer unless they apply for permission from the court to do so.¹¹⁵ The most that an appellant will receive by way of disclosure is the “gist” of the case against them.¹¹⁶
- 68.** CMPs have raised considerable concerns from many quarters and JUSTICE labelled the procedure “inherently unfair” in briefings to Parliament during the passage of the Justice and Security Bill.¹¹⁷ The former President of the Supreme Court, Lord Phillips, warned that “familiarity with the use of such a procedure will sedate those who use it against the abhorrence that the need to resort to such means should provoke.”¹¹⁸ Further, when discussing CMPs in *Bank Mellat (No. 1)*, Lord Neuberger stated that “every party has a right to know the full case against him, and the right to test and challenge that case fully”.¹¹⁹ However, noting the 2013 Act, he conceded that the “courts are obliged to apply the law in this area, as in any other area, as laid down in statute by Parliament” unless it infringes upon article 6 rights.¹²⁰
- 69.** Where the civil courts receive an application for a section 6 declaration under the 2013 Act, it is unclear how critically judges review the application and this is an issue that merits further research.¹²¹ Lord Justice Richards suggested in *McGartland* that the judiciary take their duty to review a declaration, pursuant to section 7, seriously.¹²² However, the decision in *McGartland* raises the possibility that courts will rely more heavily on CMPs where there is an NCND response. From our research, we have encountered concerns that judges may grant section 6 applications in order to view more material and evidence that might not be revealed in open or private hearings.

¹¹³ Section 9 Justice and Security Act 2013.

¹¹⁴ CPR, Rule 82.11

¹¹⁵ *Ibid.*

¹¹⁶ Please note that the Bingham Centre for the Rule of Law is looking at ‘Opening up closed judgments: balancing secrecy, security and accountability.’ See <https://www.biicl.org/binham-centre/projects/closedjudgments>.

¹¹⁷ JUSTICE, ‘Justice and Security Bill’, <https://justice.org.uk/justice-security-bill/>

¹¹⁸ Nicholas Phillips, ‘Closed Material’, London Review of Books (17 April 2014) Vol. 36, No. 8, pp. 29-32, available online at <https://www.lrb.co.uk/v36/n08/nicholas-phillips/closed-material>

¹¹⁹ See note 25, *Bank Mellat (No. 1)*, at para 3.

¹²⁰ *Ibid.*, at para 8.

¹²¹ *Secretary of State for the Home Department v AF, AN and AE (No. 3)* [2009] UKHL 28. The ruling took into account the decision in *A v UK* [2009] ECHR 301 at para 220, where the European Court of Human Rights considered the special advocate procedure. Lord Hope said at para 85 that the applicant “must be given sufficient information to enable his special advocate effectively to challenge the case that is brought against him.” Goss explains that in the more recent case of *Home Office v Tariq* [2011] UKSC 35, “the gisting requirement was enforced less rigorously in a security-vetting case where the applicant’s liberty was not at stake.” (Ryan Goss, ‘Secret Evidence and Closed Material Procedures’, in Liora Lazarus, Christopher McCrudden, Nigel Bowles (eds.), *Reasoning Rights: Comparative Judicial Engagement* (Hart Publishing, 2014), p. 130).

¹²² See note 12, *McGartland*, at para 48.

- 70.** Although we maintain that CMPs are flawed and constitute a serious barrier to access to justice, such procedures show no sign of being removed or replaced. As a consequence, we emphasise that the presumption should be that cases involving sensitive information be resolved through a PII process rather than closed proceedings. PII can effectively protect information in the interests of national security and serves the interests of justice to a much greater extent than a CMP.¹²³

- 71.** Where there are applications for closed proceedings, the parties and the courts must be more vigilant in ensuring that NCND is not unduly relied upon. In the recent case of *Belhaj*, which also concerned allegations of extraordinary rendition, Mr Justice Popplewell observed:

*I have not lost sight of the fact that it would have been possible for the Defendants to submit a draft closed Defence in the closed material in support of this application, or at least a document identifying whether any admissions would be made and what positive case would be run in relation to the core factual narrative. That would have enabled the Court to assess the issues without the need for the Defendants to rely on NCND or to avoid identifying their positive case in relation to the core narrative.*¹²⁴

- 72.** It is unsatisfactory that reliance was placed on NCND in a case such as this. The State party should be considering initiatives to avoid NCND at an early stage of the proceedings rather than at a late stage, or not at all. Furthermore, Mr Justice Popplewell granted the section 6 application despite the large quantity of material available in the public domain and the fact that “many key facts in the case and of the CIA rendition programme in general are officially confirmed.”¹²⁵

Assumed Facts

- 73.** Although we agree with Liberty that there should be a presumption in favour of open proceedings at the IPT,¹²⁶ we note that the IPT, to its credit, tries to avoid closed hearings and has facilitated open hearings by conducting cases based on “assumed facts”.¹²⁷

¹²³ See Reprieve’s discussion of the effectiveness of PII and the ‘myth’ of leaky cases perpetuated by the security services to justify going into a closed hearing. Reprieve, ‘Public Interest Immunity and *Binyam Mohamed*’ (27 March 2013), available online at http://www.reprieve.org.uk/wp-content/uploads/2014/10/2012_03_27_PUB_Briefing_on_PII_in_Binyam_Mohamed.pdf

¹²⁴ See note 103, *Belhaj v Straw*, at para 50.

¹²⁵ Reprieve, ‘Jack Straw MI6 Rendition Trial to be Heard in Secret’ (21 July 2017), available online at <https://www.reprieve.org.uk/press/jack-straw-mi6-rendition-trial-heard-secret/>

¹²⁶ Liberty, ‘Liberty’s submission to the Review of Terrorism’s Investigatory Powers Review’ (November 2014), at para 51, available online at <https://www.liberty-human-rights.org.uk/sites/default/files/Liberty%20submission%20to%20the%20Review%20of%20Communications%20Data%20and%20Interception%20Powers%20%28Nov%202014%29.pdf>

¹²⁷ In this section, we have drawn from forthcoming academic research carried out by former policy intern at JUSTICE and doctoral student at University College London, Daniella Lock.

74. The President of the Tribunal, Sir Michael Burton, explained the process of holding an open hearing based on assumed facts in *Privacy International and Others v Secretary of State for Foreign and Commonwealth Affairs and Others*:

*The now well established procedure for this Tribunal is to make assumptions as to the significant facts in favour of claimants and reach conclusions on that basis, and only once it is concluded whether or not, if the assumed facts were established, the respondent's conduct would be unlawful, to consider the position thereafter in closed session.*¹²⁸

75. However, the IPT also explained that this procedure allows it to preserve the respondent's reliance on NCND.¹²⁹ Therefore, conducting cases based on assumed facts rather than going into a closed hearing gives rise to greater use of NCND.

76. Although, given the circumstances, we welcome a process that encourages open hearings, there are situations where relying on "assumed facts" leads to absurdity. For instance, the security services maintain an NCND response in relation to many of the revelations from the Snowden leaks. As one of our consultees observed, this does not prevent those who would harm the UK's national security from accessing the content of the documents online. Therefore, it seems clear that public authorities overuse the response to the detriment of the complainant when the information they seek to avoid disclosing is widely available on the internet.¹³⁰

77. This was the situation in *Privacy International and Others v Secretary of State for Foreign and Commonwealth Affairs and Others* concerning GCHQ's hacking capabilities, as revealed by Edward Snowden. On the particular issue of whether GCHQ carries out Computer Network Exploitation (CNE), the claimants drew attention to the fact that the Intelligence Services Commissioner (ISC) published a report explicitly referring to CNE operations in March 2015. They argued that it was an "improper and over-broad national security claim" to neither confirm nor deny CNE when details about the operation were included in the ISC report and were therefore "officially confirmed".¹³¹

78. Irrespective of any other standards applied to assess the use of NCND, we consider it wholly inappropriate for public authorities to be allowed to rely on an NCND response where information has been placed in the public domain and officially confirmed.¹³² We

recommend that there should be no "assumed facts" procedure where there are "known facts" confirmed by officials or through official documentation.

79. Where there is an oral hearing that relies on "assumed facts", we recommend that the Tribunal require the parties to the litigation to draw up a "Schedule of Avowals". Such a Schedule was produced by the claimants in the GCHQ hacking case, discussed above.¹³³ The avowals determined areas of acceptance between the claimants and respondents and provide a useful model for the conduct of cases so as to minimise the need for assumed facts or NCND. The Tribunal should encourage parties to cooperate and use the assistance provided by Counsel for the Tribunal to agree a "List of Issues" to be resolved at the hearing.¹³⁴

¹²⁸ See note 91, at para 2.

¹²⁹ *Ibid.*

¹³⁰ This criticism has also been made in other jurisdictions. For example, in the US the CIA repeatedly responded with NCND in relation to its torture and rendition programme. As OPBP explains: "the CIA was selectively leaking information to journalists but ensuring that the person giving information could not be attributed to a member of the CIA so they would not have to disclose under the official acknowledgment doctrine." (See Annex I, at p. 28.)

¹³¹ [2016] IPT/14/85/CH, the Claimant's Reply, available online at http://www.ipt-uk.com/docs/Privacy_Greenet_and_Sec_of_State.pdf.

¹³² See also Annex I, at p. 13.

¹³³ See note 91, *Privacy International v Secretary of State for Foreign and Commonwealth Affairs*, at para 5.

¹³⁴ *Ibid.*, at para 8.

V. The Investigatory Powers Tribunal

80. The Investigatory Powers Tribunal (IPT) was established under Part 4 of RIPA to consider and determine complaints that allege unlawful interception of communications by public authorities and law enforcement agencies and to exercise jurisdiction over the Agencies for all proceedings under the Human Rights Act 1998.¹³⁵ Therefore, the IPT takes on an investigative function as well as fulfilling a judicial function. It is not part of Her Majesty's Courts and Tribunals Service (HMCTS).

Rules

81. The IPT is not subject to the Civil Procedure Rules (CPR). Instead, it is entitled to determine its own procedure in relation to any proceedings, complaint or reference subject to rules made by the Secretary of State.¹³⁶ Its rules were established in 2000 under section 69 RIPA via a statutory instrument.¹³⁷ The IPT website explains that the rules relate to:

- *How the Tribunal should proceed in its investigations and determinations;*
- *How it should receive evidence;*
- *In what circumstances it may disclose material provided to it;*
- *How it should determine proceedings, including oral hearings; and*
- *How it should notify a complainant of the outcome.*¹³⁸

82. However, the rules offer scant detail and place few duties on the Tribunal. For example, the Tribunal is under no duty to hold hearings, there is no requirement that complainants have the opportunity to make submissions and complainants are not entitled to an *inter partes* hearing.¹³⁹

83. The absence of adequate procedures to govern hearings has created a situation where the odds are stacked against a complainant.¹⁴⁰ As mentioned in JUSTICE's 2009, 2011 and 2015 reports, the lack of detailed procedures negates the Tribunal's attempts to improve transparency and instil confidence in its decision-making.¹⁴¹ Within this context, NCND poses yet another threat to open justice by restricting a complainant's access to information and, thereby, potentially undermines the Article 6 ECHR right to a fair trial.

¹³⁵ Section 65.

¹³⁶ Section 68, RIPA 2000.

¹³⁷ The Investigatory Powers Tribunal Rules 2000 (SI 2000/2665). The IPT recently issued draft rules and opened a consultation on the new rules, see <https://www.gov.uk/government/consultations/investigatory-powers-tribunal-consultation-updated-rules>

¹³⁸ <http://www.ipt-uk.com/content.asp?id=18>

¹³⁹ See note 3, *Freedom from Suspicion* (2011) at para 370. See also note 126, 'Liberty's submission', at para 51.

¹⁴⁰ *Ibid.*, at paras 357-369.

¹⁴¹ *Ibid.*, at paras 369-370 and note 4, *Freedom from Suspicion* (2015), at para 41.

84. Despite these barriers, the IPT concluded in *Belhadj* that the NCND policy is consistent with RIPA and the rules of the IPT. Specifically, the Tribunal found the policy is consistent with rule 6; which places a duty on the IPT to avoid disclosing information that is contrary to the public interest or prejudicial to national security.¹⁴² The same judgment referred to the European Court of Human Rights (ECtHR) ruling in *Kennedy v UK* which stated that rule 6 on disclosure, and the associated NCND response, is compatible with article 6 ECHR because the prohibition on disclosure is not absolute.¹⁴³

85. However, our 2011 report argued that:

The ultimate compatibility of the Tribunal and RIPA as a whole with the requirements of Articles 8 and 6 of the Convention remains very much in doubt ... there are compelling grounds for the view that Kennedy was wrongly-decided...¹⁴⁴

86. Reasons for doubting the *Kennedy* decision include concerns over the IPT's ability to "effectively check abuse of surveillance powers by public authorities."¹⁴⁵ The revelations from the Snowden leaks strongly suggest that the IPT has not acted as an effective bulwark against disproportionate and unlawful surveillance.¹⁴⁶ In November 2017, the ECtHR heard the case of *Big Brother Watch and others v UK*¹⁴⁷ concerning the UK's surveillance regime (as revealed by the Snowden leaks). As part of the complaints, some of the applicants challenged the compatibility of the IPT's procedures with Article 6 ECHR. Therefore, the Tribunal's effectiveness in ensuring access to justice is once more under scrutiny.

87. Currently, the Tribunal's rules and procedures are not suited to challenging public authorities when they rely on NCND. As stated in our 2011 and 2015 reports, the Tribunal should adopt fair procedures, including rules on a right to an oral hearing, disclosure of evidence, cross examination of witnesses and the giving of reasons.¹⁴⁸

Sanctions for Failure to Disclose

88. We have already discussed the need for the IPT to have more explicit powers to order disclosure. The IPT should use its powers to, exceptionally, sanction the parties for avoiding or delaying disclosure. Our 2011 report commended the IPT for refusing a

¹⁴² See note 46, *Belhadj v Security Service*, at paras 21-23.

¹⁴³ (2011) 52 EHRR 4, at para 187; the effect of rules relating to closed hearings was raised in *Belhadj* by the claimants, however the court decided that it was not the appropriate time to consider the rules. *Ibid.*, at paras 23-33.

¹⁴⁴ See note 3, *Freedom from Suspicion* (2011), at para 377.

¹⁴⁵ *Ibid.* See also Lord Kerr's dissent in *Home Office v Tariq* [2011] UKSC 35 and JUSTICE's intervention in that case, available online at <https://2bqk8cdew6192tsu41lay8t-wpengine.netdna-ssl.com/wp-content/uploads/2015/01/Written-submission-in-Tariq-v-UK-at-ECtHR.pdf> and note 95, the Bingham Centre for the Rule of Law's submission, at paras 48-51.

¹⁴⁶ Our 2011 report made this point prior to the Snowden revelations. See note 3, *Freedom from Suspicion* (2011), at para 369. This concern has been raised post the revelations, see note 126, 'Liberty's submission', at para 50.

¹⁴⁷ App. No. 58170/13.

¹⁴⁸ See note 3, *Freedom from Suspicion* (2011) at para 400, and note 4, *Freedom from Suspicion* (2015) at para 36. See also note 126, 'Liberty's submission', at para 51.

public authorities' application for an award of costs against the complainant after they withdrew their application.¹⁴⁹ The judgment concluded that "it would appear from the statute [RIPA 2000] that the Tribunal was intended to be cost-free to the complainant".¹⁵⁰ The IPT can therefore award costs in the complainant's favour, and did so in the 2015 case of *Chatwani*,¹⁵¹ which is the only occasion where the IPT has taken this measure.

- 89.** The case concerned the installation of covert listening devices at the complainants' offices and headquarters. The complainants sought a declaration that the authorisation for property interference was unlawfully obtained and sought a return of the material obtained. The Tribunal emphasised that the respondent was under a "duty of candour"¹⁵² when it made an application for a search warrant. The respondent was as a result obliged to make full and accurate disclosure to enable an officer who is authorised to interfere with property to give their approval.¹⁵³ The Tribunal found that the respondent failed to record that there was a likelihood of legally and professionally privileged material being captured on covert listening devices.¹⁵⁴ It decided not to make an award of costs in the complainant's favour as the representative could not draw attention to a previous decision or rule allowing it to do so and legal costs were not a recognised head of damages.¹⁵⁵ However, according to the IPT's 2016 report, costs were awarded to the complainant at a later stage due to the respondent's failure to comply in a timely fashion with the Tribunal's orders.¹⁵⁶
- 90.** We consider that the approach to disclosure by the State party warrants greater scrutiny. The current approach exacerbates the already existing inequality of arms between the parties. To deter the respondent from making late disclosures, we recommend that the IPT use its powers to issue costs orders in extreme cases, as was done in *Chatwani*. This could be done in a similar fashion to an indemnity basis costs order in the civil courts: any doubt would be resolved in favour of the receiving party¹⁵⁷ and an order would only be issued

in rare circumstances based on some conduct or circumstance "which takes the case out of the norm."¹⁵⁸

- 91.** Issuing costs orders in the IPT in rare circumstances would deter the State party from attempting to use NCND as a tool for avoiding disclosure and gaining a litigation advantage over the complainant. While this may raise risks for the complainant,¹⁵⁹ such a costs regime should be aimed at unjustified late disclosure and take into account the duty of candour held by public authorities involved in litigation.

Case Outcomes

- 92.** IPT rule 13(2) states that where the Tribunal makes a determination in favour of a complainant it "shall provide him with a summary of that determination including any findings of fact."¹⁶⁰ This is subject to the general duty under rule 6(1) to avoid disclosing sensitive information. Where it finds in favour of the complainant the IPT must state that it has done so, thus breaching NCND, though it does not give details of the unlawful conduct. This constitutes an important statutory exception to NCND. However, a Tribunal's "no determination" constitutes an NCND response as it would not, for example, disclose whether a complainant has or has not been under surveillance.¹⁶¹ This presumes that, as one of our consultees explained: NCND is maintained when the intelligence community or an agent has acted lawfully, but is not maintained when they have acted unlawfully.
- 93.** The Tribunal confirmed in *Belhadj* that NCND has a role to play after a successful complaint and that the giving of information to the complainant is additional to the determination required under s. 68(4) RIPA 2000.¹⁶² It is for the Tribunal to consider whether "supplying such *additional* information" complies with its duty under Rule 6(1) to protect sensitive information in the public interest.¹⁶³ However, the Tribunal emphasised that:

*NCND is not in itself a statutory rule. It is s.69(6)(b) and Rule 6(1), made consistently with that section, which require the Tribunal to give respect to the NCND principle, but in our judgment Rule 6(1) does not go so far as to empower the Tribunal not to disclose to a complainant, in a case where unlawful conduct has been found, even the fact that the complaint has been determined in his favour.*¹⁶⁴

¹⁴⁹ See note 3, *Freedom from Suspicion* (2011), at para 367.

¹⁵⁰ *W v Public Authority* [2011] UKIPTrib 09/134/C, at para 8.

¹⁵¹ *Chatwani & Others v National Crime Agency* [2015] UKIPTrib 15/84/88/CH.

¹⁵² The 'duty of candour' in judicial review proceedings holds public authorities to account for failure to disclose. As with cases in the IPT, judicial review proceedings are not subject to the rules of disclosure in the CPR. To ensure that the appropriate facts come to light in judicial review cases, the duty requires public authorities to make a candid disclosure of its decision-making process. When assessing whether to issue an order for disclosure, the court will have regard to whether it is necessary "to resolve the matter fairly and justly," (see *Tweed v Parades Commission* [2006] UKHL 53, at paras 2-3). If the public authority fails to comply with the duty of candour, the court may draw inferences and it may lead to the court granting applications for specific disclosure of particular documents. (See Lord Chief Justice of England and Wales, 'Defendant's Duty of Candour and Disclosure in Judicial Review Proceedings: A Discussion Paper' (28 April 2016), at paras 14-15, available at <https://www.judiciary.gov.uk/wp-content/uploads/2016/04/consultation-duty-of-candour-april-2016.pdf>)

¹⁵³ See note 151, *Chatwani*, at para 15.

¹⁵⁴ *Ibid.*, at para 43.

¹⁵⁵ *Ibid.*, at para 48.

¹⁵⁶ See note 49, 'Report of the Investigatory Powers Tribunal: 2011-2015', at para 5.10.

¹⁵⁷ CPR 44.3(3).

¹⁵⁸ Per Lord Woolf, Lord Chief Justice, as he then was, in *Excelsior Commercial & Industrial Holdings Ltd v Salisbury Hamer Aspden & Johnson (Costs)* [2002] EWCA Civ 879, at para 19.

¹⁵⁹ See note 3, *Freedom from Suspicion* (2011), at para 367 in reference to *W v Public Authority* (IPT/09/134/C/1): "the prospects of complainants before the Tribunal are dim enough without the additional threat of an adverse costs order to dissuade them further."

¹⁶⁰ See note 137, IPT Rules 2000.

¹⁶¹ See also the preliminary ruling in *B v Security Service* IPT/03/01/CH, 31 March 2003 which concerned the Security Service's interference with article 8 ECHR rights and the discussion in JUSTICE, *Freedom from Suspicion: Surveillance Reform* (2011), at paras 371-372.

¹⁶² See note 46, *Belhadj v Security Service*, at para 21.

¹⁶³ *Ibid.*

¹⁶⁴ *Ibid.*

- 94.** However, we understand that successful complainants often receive inadequate reasons for a decision. For instance, the determination in favour of the Legal Resources Centre and Amnesty international in *Liberty/Privacy (No. 2)* offered scant detail about the unlawful conduct that took place.¹⁶⁵ The position is even worse for unsuccessful complainants, as noted above. Liberty has explained:

*If the Tribunal finds against a complainant it cannot give its reasons for doing so, meaning that the individual does not know whether no surveillance took place or whether lawful surveillance took place, and if it upholds a complaint is it [sic] only required to provide the complainant with a summary of its reasoning.*¹⁶⁶

- 95.** The limited explanation of the reasons for a decision therefore prevents access to meaningful justice because it is not clear to complainants why a decision has been reached.
- 96.** We recognise the difficulty of explaining decisions in the context of sensitive information. However, we contend that IPT rule 13(2) can be interpreted more widely to give fuller detail than is currently being provided. In this respect, the IPT could look to other jurisdictions, such as Special Immigration Appeals Commission (SIAC), which encounters secret evidence but is able to produce written reasons.¹⁶⁷

VI. Accountability

Appeals

- 97.** In our 2015 report, we recommended a right of appeal from the IPT.¹⁶⁸ At the time of writing, there is still no domestic route for an appeal or review from the IPT.¹⁶⁹ Although section 242 of the Investigatory Powers Act 2016 sets out a right of appeal on a point of law,¹⁷⁰ this has not yet been brought into force. The Government's impact assessment noted:

*It is important for public trust and confidence in the use of investigatory powers that there is a robust means by which the use of these sensitive investigative techniques use [sic] can be challenged.*¹⁷¹

- 98.** This contrasts with the situation in Canada. A statutory review and appeals system may be invoked where an individual encounters an NCND response to an Access to Information request.¹⁷²
- 99.** The appeal mechanism must be brought into force as soon as possible.¹⁷³

Oversight Mechanisms

- 100.** Currently, public authorities do not publish details of how often they use an NCND response. The Government could help to demystify the NCND policy by detailing the frequency of responses to access to information requests under the Freedom of Information Act and the Data Protection Act at least annually.¹⁷⁴ This is a measure already taken in Canada and the figures are published in an annual report.¹⁷⁵ OPBP notes:

As governmental bodies [in Canada] also have to report the use of NCNDs, there is a system for accountability in place within the government. Furthermore, government

¹⁶⁵ See note 48, *Liberty/Privacy (No. 2)* and the 'Amended Open Determination' available online at http://www.ipt-uk.com/docs/Final_Liberty_Ors_Open_Determination_Amended.pdf

¹⁶⁶ See note 3, *Freedom from Suspicion* (2011), at para 400, and note 4, *Freedom from Suspicion* (2015), at para 36. See also note 126, 'Liberty's submission', at para 51.

¹⁶⁷ We note that rule 15 of the Investigatory Powers Tribunal Draft Rules provides for further information than previously required in relation to a determination by the Tribunal.

¹⁶⁸ See note 4, *Freedom from Suspicion* (2015), at paras 39-41.

¹⁶⁹ It is therefore only possible to challenge a ruling by making an application to the ECtHR.

¹⁷⁰ In *R (Privacy International) v Investigatory Powers Tribunal* [2017] EWHC 114 (Admin), Privacy International challenged the IPT's contention that section 67(8) RIPA amounted to an ouster clause. At para 35, Sir Brian Leveson P described how the problems created in this case "will, for the future, be avoided and, if leave be granted, an appeal from one of the IPT's decisions could in future be mounted through the relevant appellate courts."

¹⁷¹ Home Office, 'Impact assessment: Investigatory Powers Tribunal' (7 July 2016), at A.1, available online at https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/536330/impact-assessment-investigatory-powers-tribunal.PDF

¹⁷² Annex 1, p. 9, 15-17. See also Annex 2, pp. 12-14: a review may be undertaken by Canada's Federal Court and may be conducted in camera. It seems that principles of Canadian administrative law and the duty of procedural fairness would apply in the circumstances.

¹⁷³ Based on our consultation, it is our understanding that the provision will be brought into force shortly.

¹⁷⁴ One of our consultees suggested that this information could be included in the Home Office's Transparency Report. See Home Office, *HM Government Transparency Report 2017: Disruptive and Investigatory Powers* (February 2017), available online at <https://www.gov.uk/government/publications/disruptive-and-investigatory-powers-hm-government-transparency-report>

¹⁷⁵ See, for example, Treasury Board Secretariat, *Access to Information Act Annual Report 2016-2017*, (2017) available online at <https://www.canada.ca/en/treasury-board-secretariat/corporate/reports/access-information-privacy-reports-treasury-board-secretariat/2016-17-annual-report-access-information-act.html>

*departments and institutions may have their own ombudsman or watchdog that may consider NCND issues in the context of their institutions.*¹⁷⁶

101. To institute greater accountability, we recommend that the UK follow Canada's example and establish a system of accountability within Government. However, Canada lacks an overall body that is specifically responsible for reviewing the NCND responses of the Canadian Government and intelligence agencies.¹⁷⁷ We consider that a specific oversight body should be charged with considering NCND responses. In our 2015 report, we recommended the creation of a single, streamlined body to oversee the use of surveillance powers by public bodies reflecting, to various extents, recommendations by the previous Independent Reviewer for Terrorism Legislation¹⁷⁸ and recommendations by a Royal United Services Institute panel in 2015.¹⁷⁹ We considered a single body to be advantageous as it would combine "all the relevant expertise" to "provide effective scrutiny in this fast-changing field."¹⁸⁰

102. We welcome the creation of the Investigatory Powers Commissioner's Office (IPCO) – which has replaced the separate posts of surveillance commissioner, interception of communications commissioner and intelligence services commissioner – under the Investigatory Powers Act 2016.¹⁸¹ IPCO must be well-resourced and given sufficient access to information to carry out its role effectively.¹⁸² In relation to NCND, we suggest that IPCO be tasked with monitoring and reporting the response as part of the "additional directed oversight functions" under the Act, which requires the Commissioner to

... keep under review the carrying out of any aspects of the functions of –

i. an intelligence service,

¹⁷⁶ Annex I, p. 34.

¹⁷⁷ *Ibid.*

¹⁷⁸ See note 81, David Anderson QC, *A Question of Trust*, at para 14.94.

¹⁷⁹ RUSI, *A Democratic Licence to Operate: Report of the Independent Surveillance Review* (July 2015), recommendations 17-18, available online at https://rusi.org/sites/default/files/20150714_whr_2-15_a_democratic_licence_to_operate.pdf

¹⁸⁰ See note 4, *Freedom from Suspicion* (2015), at para 47.

¹⁸¹ Section 227. The first Investigatory Powers Commissioner, Lord Justice Fulford, was appointed on 3 March 2017 for a three-year term, see GOV.UK, 'Investigatory Powers Commissioner appointed: Lord Justice Fulford', (3 March 2017) available online at <https://www.gov.uk/government/news/investigatory-powers-commissioner-appointed-lord-justice-fulford> Note also, the former Independent Reviewer of Terrorism Legislation's criticism of the Act: "An opportunity was missed to recognise in statute what will surely be known as the *Investigatory Powers Commission*, and to reflect in its name the reality that its functions extend to intelligence supervision even outside the area of investigatory powers." Independent Reviewer of Terrorism Legislation, 'The Investigatory Powers Act 2016 – an exercise in democracy', (3 December 2016, edited 26 June 2017) available online at <https://www.daqc.co.uk/2016/12/03/the-investigatory-powers-act-2016-an-exercise-in-democracy/>

¹⁸² It is encouraging to note that the Investigatory Powers Commissioner has emphasised that all relevant persons have a statutory duty under the Act "to provide my office with all information necessary to enable us to carry out our oversight function." (See the 'Open Response' from the Rt. Hon. Lord Justice Fulford, the Investigatory Powers Commissioner, to the letter of 13 September 2017, available online at <https://ipco.org.uk/docs/2017%2010%2013%20IP%20Commissioner%20response%20to%20Privacy%20International%20et%20al.pdf>) However, we are concerned that the intelligence agencies have not made sufficient disclosure in relation to their activities. (See, Privacy International, 'Disclosure and documents received for Bulk Personal Datasets Challenge: October 2017, available online at <https://privacyinternational.org/node/1532>).

ii. a head of an intelligence service, or

*iii. any part of Her Majesty's forces, or of the Ministry of Defence, so far as engaging in intelligence activities.*¹⁸³

103. We also recommend that Parliament's Intelligence and Security Committee has oversight of the NCND response.¹⁸⁴ The members of the committee already have the advantage of being security-cleared to view sensitive information. Through its expanded role following the passage of the Justice and Security Act 2013,¹⁸⁵ the Committee could offer a different perspective to the judiciary and the commissioners and provide greater accountability.

104. The IPT itself must do more to improve public accountability and promote trust in its procedures. In 2013, the President of the IPT, Mr Justice Burton, said at a meeting of the Public Law Project that the IPT would be willing to consider public listings of tribunal hearings on the IPT's website.¹⁸⁶ At the time of writing, listings are inconsistently provided on the website and public access to the Tribunal remains challenging – even if hearings are open to the public.¹⁸⁷ Phil Chamberlain, a journalist, explained that to attend a hearing he needed to be briefed by the claimants (Privacy International).¹⁸⁸ They directed him to the Tribunal's hearing at the Rolls Building in London and he described finding the hearing as "more akin to finding a rave in the 1980s."¹⁸⁹ The difficulties in accessing the IPT contradicts the statement on its website that it operates "the most open and equitable process in the world for hearing cases of this sensitivity."¹⁹⁰ We therefore recommend hearings at the IPT always be listed publicly and well in advance, and a clear indication be given of where hearings will be held.

105. In addition, the IPT can improve public accountability by reporting annually on developments and how it fulfils its role. To date, there have only been two reports by the IPT and the sections on "Neither Confirm Nor Deny" within each report neglect to offer a satisfying account of the IPT's interaction with NCND and how it scrutinises the policy. Instead, they are limited to explaining the rationale underpinning NCND and the tribunal's remit.¹⁹¹

¹⁸³ Section 230(1).

¹⁸⁴ For a discussion of the Intelligence and Security Committee and its role in overseeing the Agencies, see Hugh Bochel, Andrew Defty and Jane Kirkpatrick, "'New mechanisms of independent accountability': select committees and parliamentary scrutiny of the intelligence services", *Parliamentary Affairs*, Vol. 68(2) (2015), pp. 314-331.

¹⁸⁵ The committee's remit was extended to operational activity and the wider intelligence and security activity of the Government. See House of Commons Library, 'The Intelligence and Security Committee' (14 June 2017), available online at <http://researchbriefings.parliament.uk/ResearchBriefing/Summary/SN02178>

¹⁸⁶ Owen Bowcott, 'Surveillance tribunal may allow publicity', *The Guardian* (14 October 2013).

¹⁸⁷ Judith Townend, 'Justice must be seen to be done. But what does that mean?', *Proof Magazine*, (9 February 2017), available online at <http://thejusticegap.com/2017/02/proof-magazine-justice-must-be-seen-done/>

¹⁸⁸ Phil Chamberlain, 'Open Justice? You'll Have to Find us First', *Proof Magazine*, (No. 2, 2 January 2017), pp. 48-51.

¹⁸⁹ *Ibid.*, p. 50.

¹⁹⁰ <http://www.ipt-uk.com/default.asp>

¹⁹¹ <http://www.ipt-uk.com/content.asp?id=33>

Expertise and Special Counsel

106. The IPT differs from other civil courts and SIAC in having a “Counsel to the Tribunal” rather than a Special Advocate. The Counsel to the Tribunal performs a role “akin to that of *amicus curiae*” and assists the tribunal “in whatever way the tribunal directs”,¹⁹² unlike a Special Advocate who is necessarily partisan.

107. In the case of *Liberty/Privacy (No. 1)*, the Tribunal agreed with the Counsel to the Tribunal’s submission that it could best assist:

*[B]y performing the following roles: (i) identifying documents, parts of documents or gists that ought properly to be disclosed; (ii) making such submissions to the Tribunal in favour of disclosure as are in the interests of the Claimants and open justice; and (iii) ensuring that all the relevant arguments on the facts and the law are put before the Tribunal. In relation to (iii), the Tribunal will expect its counsel to make submissions from the perspective of the Claimants’ interests (since the Respondents will be able to make their own submissions). If the Tribunal decides to receive closed oral evidence from one or more of the Respondent’s witnesses, it may also direct its counsel to cross-examine them. In practice, the roles performed by counsel to the Tribunal at this stage of the current proceedings will be similar to those performed by a Special Advocate in closed material proceedings.*¹⁹³

108. We consider that Counsel to the Tribunal will play a valuable role in IPT appeals, should an appeal mechanism be brought into force. Our consultation revealed that Counsel to the Tribunal serves a useful function already, particularly in closed hearings. They have a greater ability to communicate with the claimant after viewing closed material than Special Advocates. However, as our 2015 report argued, although Counsel to the Tribunal plays a valuable role, “it is not an effective substitute [for special advocates] because counsel to the Tribunal is not charged with representing the interests of the excluded party and, in the *Liberty* case, took no instructions from the excluded parties.”¹⁹⁴

109. From our research we have also found that the IPT would be well served by having expertise on its panel.¹⁹⁵ This would allow the Tribunal to be empowered in its assessment of an NCND response. In this regard, the Tribunal could again emulate SIAC.

110. SIAC considers appeals against a decision under Part IV of the Immigration and Asylum Act 1999.¹⁹⁶ The Commission is composed of judicial members, legal members and expert

lay members. For example, the expertise of former head of MI5, Sir Stephen Lander, was instrumental in finding that the former aide of Mike Hancock MP, who had a four year affair with the politician, was not a spy. In fact, Mr Justice Mitting noted in his judgment that Lander’s presence was “essential to permit us [the SIAC panel] to reach a sound and just decision.”¹⁹⁷ We recommend that relevant specialist expertise be included amongst the tribunal members. Where necessary, we also suggest that the IPT could instruct experts to advise it on specific technical issues that may arise. The kind of specialisms which might particularly benefit the IPT include expertise on modern surveillance techniques, and experience in minimising privacy intrusions.

¹⁹² See note 47, *Liberty/Privacy (No. 1)*, at para 8.

¹⁹³ *Ibid*, at para 10.

¹⁹⁴ See note 4, *Freedom from Suspicion* (2015), at para 41.

¹⁹⁵ Submissions to the Independent Reviewer of Terrorism Legislation’s review also recommended the introduction of “expert technological expertise”, see note 81, David Anderson QC, ‘A Question of Trust’, at para 12.89.

¹⁹⁶ With limited exceptions - Section 2(1), Special Immigration Appeals Commission Act 1997: “A person may appeal to [SIAC]...but for a public interest provision”. [Emphasis added] The section explains that a public interest provision means “any of sections 60(9), 62(4), 64(1) or (2) or 70(1) to (6)” of the Immigration Act 1999.

¹⁹⁷ *Zatuliveter v Secretary of State for the Home Department* [2011] UKSIAC 103/2010, at para 30.

VII. Conclusion

- 111.** Ambiguity surrounding the neither confirm nor deny response has fostered a culture of secrecy that enables public authorities to avoid facing proper accountability for alleged unlawful activity. NCND can be a legitimate response to protect national security when used appropriately. However, overuse of the response by public authorities, and the judiciary's deference to national security arguments, hinders access to justice. It must not be used as a blanket response to defeat a claim or unduly restrict disclosure.
- 112.** The lack of a coherent NCND policy has compelled the courts to determine cases that rely on the NCND response without proper guidance. This has undermined the ability of the civil courts and the Investigatory Powers Tribunal to make judgments based on a coherent policy.
- 113.** In tandem, the civil courts and the IPT have often been timid in their scrutiny of NCND. Although the civil courts and the IPT consider the competing public interests in disclosing information and maintaining confidentiality, they have refrained from establishing and applying a consistent standard. We believe the court can, and should, take a more rigorous approach.

VIII. Recommendations

Disclosure

- 1.** Public authorities should conduct case-by-case assessments of the risk in disclosing sensitive information.
- 2.** Public authorities should provide written reasons for relying on the NCND response each time it is used.
- 3.** The Investigatory Powers Tribunal (IPT) should have an explicit power to order disclosure to non-State parties, and this should be enshrined in the Tribunal's rules.

Policy

- 4.** The Government should produce a clear and coherent NCND policy that is easily accessible.
- 5.** The NCND policy should reflect the European Convention on Human Rights proportionality test.

Judicial Scrutiny

- 6.** The judiciary should consistently subject the NCND response to a balance of interests test.
- 7.** The judiciary should be rigorous in its assessment of NCND and demand detailed and specific reasons when a public authority invokes the response.
- 8.** There should be a presumption that cases that rely on sensitive information be resolved through a Public Interest Immunity process rather than a Closed Material Procedure.
- 9.** The State party to litigation should take all possible measures to avoid relying on NCND.
- 10.** There should be a presumption in favour of open hearings at the IPT.
- 11.** The public authorities should not be able to rely on NCND where they have placed information in the public domain.
- 12.** In the IPT there should be no reliance on "assumed facts" where the facts have been confirmed by an official authority.
- 13.** A "Schedule of Avowals" should be introduced in all cases that rely on assumed facts.

The Investigatory Powers Tribunal

- 14.** The IPT should adopt fair procedures, including rules on a right to an oral hearing, measures on disclosure of evidence and cross-examination of witnesses.

- 15. The IPT should issue costs orders where the parties avoid or unreasonably delay disclosure of information.
- 16. The IPT rule 13(2) should be interpreted more widely to allow fuller reasons for a decision.
- 17. The mechanism for domestic appeals from the IPT should be brought into force as soon as possible.

Oversight and Accountability

- 18. The Government should record and publish the frequency of NCND responses at least annually.
- 19. The Investigatory Powers Commissioner's Office should be tasked with monitoring the NCND response.
- 20. Parliament's Intelligence & Security Committee should also have oversight of the NCND response.
- 21. Hearings at the IPT should be publicly listed with a clear indication of where they will be held.
- 22. The IPT should report annually on its operations.
- 23. The IPT should introduce expertise amongst its panel members drawing from the experience of the Special Immigrations Appeals Commission.

IX. Acknowledgements

This report was written by Pouneh Ahari, Legal Researcher at JUSTICE, with oversight from Rachel Jones, Civil Lawyer and Jodie Blackstock, Legal Director.

We are very grateful to Oxford Pro Bono Publico, particularly Max Harris, Alice Irving and Dr Liora Lazarus for their research, assistance and advice. Our thanks to the University College London for kindly hosting a roundtable discussion in March 2017 and to the Bonavero Institute at the University of Oxford for hosting a further roundtable discussion in November 2017.

We would also like to acknowledge and thank the following individuals and organisations who generously gave their time to attend the roundtable discussion on the report, respond to our call for evidence, or otherwise support our work:

Dr Jessie Blackbourn, Research Fellow in the Centre for Socio-Legal Studies, University of Oxford

John Bowers QC, Principal of Brasenose College, University of Oxford

Tom Bullmore, Special Advocates' Support Office

Rosalind Comyn, Legal & Policy Officer, Rights Watch UK

Arushi Garg, Stipendiary Lecturer St. Hilda's College, University of Oxford

Camilla Graham Wood, Legal Officer, Privacy International

Jonathan Glasson QC, Matrix Chambers

The Rt. Hon. Dominic Grieve QC MP

Max Hill QC, the Independent Reviewer of Terrorism Legislation; Head of Red Lion Chambers

Dr Hayley Hooper, Pennington's Student in Law, University of Oxford

Ben Jaffey QC, Blackstone Chambers

Scarlet Kim, Legal Officer, Privacy International

Daniella Lock, University College London

Asaf Lubin, Privacy International

Annelen Micus, Head of Programmes, Bonavero Institute of Human Rights, University of Oxford

Dr Lawrence McNamara, The Bingham Centre for the Rule of Law; The University of York

Professor Catherine O'Regan, Director of the Bonavero Institute of Human Rights, University of Oxford

Ewan Smith, Shaw Foundation Junior Research Fellow at Jesus College, University of Oxford

Ashley Underwood QC, Cornerstone Chambers

Harriet Wistrich, Birnberg Peirce & Partners



JUSTICE

59 Carter Lane, London EC4V 5AQ

www.justice.org.uk