To 'Neither Confirm Nor Deny': Assessing the Response and its Impact on Access to Justice

ANNEXES

by Oxford Pro Bono Publico

JUSTICE

ANNEX I

Oxford Pro Bono Publico
www.law.ox.ac.uk/opbp

'Neither Confirm Nor Deny':

Insights from Comparative Law, Policy Bodies, and Academia

A research report by Oxford Pro Bono Publico prepared for JUSTICE

February 2016

CONTRIBUTORS

Faculty:

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

Associate Professor Liora Lazarus
Fellow at St Anne's College
University of Oxford

Research Co-ordinator(s):

Alice Irving
DPhil in Law Candidate, University of Oxford

Max Harris
All Souls College, University of Oxford

Researchers:

Rina See
Bachelor of Civil Law Candidate, University of Oxford

Alexandra Mogyros
DPhil in Law Candidate, University of Oxford

Marlena Valles
DPhil in Law Candidate, University of Oxford

Lee Jia Wei
Bachelor of Civil Law Candidate, University of Oxford

Giordana Campagna
Magister Juris Candidate, University of Oxford

Karen Staunton
Bachelor of Civil Law Candidate, University of Oxford

Paulina Fishman
MSt Legal Research Candidate, University of Oxford

Indemnity

Oxford Pro Bono Publico (OPBP) is a programme run by the Law Faculty of the University of Oxford, an exempt charity (and a public authority for the purpose of the Freedom of Information Act). The programme does not itself provide legal advice, represent clients or litigate in courts or tribunals. The University accepts no responsibility or liability for the work which its members carry out in this context. The onus is on those in receipt of the programme's assistance or submissions to establish the accuracy and relevance of whatever they receive from the programme; and they will indemnify the University against all losses, costs, claims, demands and liabilities which may arise out of or in consequence of the work done by the University and its members.

Intellectual property

The 'Neither Confirm Nor Deny' Policy: Summary of Research Findings

Oxford Pro Bono Publico has conducted research into the use of 'Neither Confirm Nor Deny' arguments, or equivalent arguments, in the United States of America, Canada, Australia, and New Zealand. We have also reviewed media discussions of 'Neither Confirm Nor Deny' ('NCND') and references to NCND in academic literature.

JUSTICE, an all-party law reform and human rights organisation working to strengthen the United Kingdom justice system, approached Oxford Pro Bono Publico to conduct comparative research on the use of 'Neither Confirm Nor Deny' policy. JUSTICE is preparing a report on NCND policy, which will include proposals for a new approach to NCND in the United Kingdom. The comparative research completed by OPBP provides material for JUSTICE to draw on in drafting their proposals, and will be an annex to the JUSTICE report upon publication.

An NCND response may be given by the government, or a government body, in many forums: it may be given by a government spokesperson in response to a question posed by a member of the media, refusing to confirm nor deny any knowledge on the matter raised; or it may be provided by a public authority in response to a freedom of information request, where they refuse to confirm nor deny that they hold the relevant information. The NCND response is utilised in circumstances where even the acknowledgment of the presence or absence of certain information would reveal sensitive or potentially damaging information. For example, the police may refuse to confirm or deny whether a person has been under surveillance, if this would reveal sensitive information about crime detection practices that may undermine ongoing investigations.

While the use of an NCND response may at times be justified, its use comes at a cost and it may be abused. JUSTICE previously raised some preliminary concerns about the use of NCND in their October 2011 report "Freedom from Suspicion: Surveillance Reform for a Digital Age". This report highlighted that while there may be a public interest in the effectiveness of surveillance and the protection of foreign intelligence material, and that these interests can be protected through the use of NCND, this comes at a cost. The use of NCND does considerable damage to principles of open justice and procedural fairness, and makes it difficult effectively to protect the right to privacy. JUSTICE noted with particular concern that the Investigatory Powers Tribunal has treated the need to preserve NCND as axiomatic to any legal framework governing the use of surveillance powers, and has been very willing to accommodate NCND responses, despite significant impact on other interests. In their 2011 report, JUSTICE questioned whether the current approach to NCND in the UK is justifiable. Their new report, to which this research will contribute, explores this issue in more detail, and will make proposals for a new approach to NCND.

In the pages that follow, we set out findings of our research into NCND policy – or its equivalent – in the United States of America, Canada, Australia, and New Zealand. We provide below a preliminary overview of some key cross-cutting themes that emerged across the individual pieces of research:

a. the criticisms that have been made of NCND;
b. the grounds on which NCND can be invoked; and
c. the need for NCND responses to be reviewed and justified, rather than automatically accepted.

Fuller references are provided in the jurisdiction-specific research briefs that follow this overview.

Criticisms of 'Neither Confirm Nor Deny' Across Jurisdictions

Objections have been directed towards the use of NCND responses in a number of the jurisdictions surveyed in this research project. The strongest objections to the use of NCND have been raised in the United States of America and in Australia, perhaps due to the relatively high use of NCND responses in these jurisdictions.

In the United States of America, particular criticism has been made of the over-use of the Glomar response – the American equivalent of NCND – in circumstances where the information in question has already entered the public domain. For example, in relation to the Torture and Interrogation Programme, the CIA were leaking information to journalists while continuing to issue a NCND response to direct queries about the programme. Similar concerns have been raised about the CIA's unwillingness to acknowledge the existence of a drone programme, or of records relating to mass-surveillance pursuant to the Snowden leaks. There has been judicial recognition, in *Public Citizen v Department of State*, of concerns that "it is unfair, and not in keeping with the [Freedom of Information Act's] intent, to permit State to make self-serving partial disclosures of classified information". Nevertheless, Edwards J concluded that such concerns should be addressed to congress, not the judiciary stating that "[i]f the legislature believes that this outcome constitutes an abuse of the agency's power to withhold documents… it can so indicate by amending the FOIA."

In Australia there has been recognition that the ongoing policy of using an NCND policy in relation to intelligence service operations significantly limits parliamentary oversight of the Australian Secret Intelligence Service. A 1994 Commission of Inquiry into the Australian Secret Intelligence Service, headed by Justice Gordon Samuels and Mr Michael Codd, criticised "the uninformative and unresponsive attitude which NCND epitomizes." While the inquiry acknowledged that "[t]here will often be circumstances, concerning operationally sensitive information or allegations, where the appropriate response from any Government will be NCND" it concluded that "if this media policy is applied in a blanket fashion, it is severely limiting". Academic commentators have noted that the use of an NCND response contributes to "[s]ubstantial inadequacies in

accountability" in the national security context, and permits the Attorney General to "control debate and accountability through selective release of information". In the context of financial regulation, the use of NCND by the Australian Securities and Investments Commission in relation to ongoing investigations has been criticised by the Governance Institute of Australia as preventing external public parties from objectively evaluating the Commission's actions. In the Freedom of Information context, in the leading authority of *Est v Department of Family Services & Aboriginal & Islander Affairs*, the Queensland Information Commissioner observed that the NCND response is open to potential misuse and should only be employed in exceptional circumstances.

In New Zealand there has been less extensive use of NCND. It has most often been used in the surveillance context, in relation to informants or intelligence capabilities. Even in this context, there has been recognition that openness is necessary to maintain public trust and that the overuse of NCND should be avoided. The former Police Commissioner Howard Broad said that the NCND policy "hasn't helped" in securing public trust for police surveillance work. Further, the New Zealand Security Intelligence Service itself has acknowledged that it is using the NCND response more broadly than it would like, because of the concern about orchestrated requests permitting people to deduce sensitive information from the pattern of responses provided. This concern has prompted proposals for a new approach, which are currently under consideration.

In Canada we have found no recent instances of the use of the NCND response in relation to a highly controversial issue. The media and news industry seem to have become accustomed to receiving NCND responses in the context of surveillance and intelligence agency matters. The availability of statutory review procedures of the use of NCND has been critical to judicial acceptance of the NCND response as necessary in certain circumstances and constitutional. In *Zanganeh v Canada Security Intelligence Service* the Court held that while Canadians may shudder to realize that the security may require utter secrecy in relation to some intelligence matters, "[w]hat no doubt distinguishes this free and democratic society from those which are less or not at all so, are the right to apply for, and obtain the results of, the Privacy Commissioner's investigation, and the right to apply to this Court for a review." Therefore, it seems that the existence of relatively robust review mechanisms contributes to a lack of controversy surrounding the use of NCND in Canada.

Therefore, it is clear that – at least in those jurisdictions where NCND responses are widely used, and where there are limited accountability mechanisms – there is significant concern about NCND policy. NCND responses can undermine public trust in security and intelligence services, and undermine the accountability of these services, in turn jeopardising basic individual rights.

The Grounds on Which NCND Can Be Invoked Across Jurisdictions

This report predominantly focuses on the use of NCND responses in the context of requests for access to official information, and in general public discourse. An

interesting allied issue, not explored in detail in this report, is the use of an NCND response in the context of civil litigation, such as a tort claim brought against a government agency. A cursory review of comments made across jurisdictions suggests that NCND ought not to be understood to give rise to immunity from tort claims.

In all of the jurisdictions surveyed, aside from the United States of America, there is a statutory basis for the use of NCND responses in the context of access to official information. In the United States of America, the Glomar response is a judicial creation. Nevertheless, its use can only be justified if it is linked to one of the Freedom of Information Act 1996 exemptions to disclosure of information. Therefore, the Glomar response is closely tethered to a legislative framework. A similar range of interests is found to justify the use of NCND across jurisdictions.

Predominantly, NCND is used in the context of national security. In the United States of America, exemptions to disclosure of information extend to cover classified documents, and that which is necessary to protect CIA sources and methods and NSA activities. Similarly, in Canada, an NCND response may be utilised where the request is related to detecting, preventing or suppressive subversive and hostile activities. New Zealand and Australia share similar statutory formulations, extending the use of NCND further still to include where it is necessary for national security and where it is necessary to prevent prejudice to international relations. However, notably, in Australia the relevant legislation – the Freedom of Information Act 1982 (Cth) – does not apply to Australian intelligence agencies. Therefore, there is no procedure allowing individual information requests from these agencies.

NCND responses are also commonly deployed in relation to law enforcement practices. In Australia and New Zealand, an NCND response may be given where this is necessary to prevent prejudice to the maintenance of law, including the prevention, investigation, and detection of offences, and the right to a fair trial. A similar exemption to disclosure exists in the Freedom of Information Act 1996 in the United States of America, and so presumably could ground the use of an NCND response. However, this has not yet been the subject of judicial consideration so far as are aware.

Beyond these two common grounds for an NCND response, there are a few other grounds that are recognised in only some of the jurisdictions surveyed. In the United States of America, an NCND response may be given where acknowledging or denying the existence of information could reasonably be expected to constitute an unwarranted invasion to the personal privacy of an individual. In New Zealand, an NCND response can be given where this is necessary to prevent endangerment of the safety of an individual. A similar exemption to disclosure of information exists in the United States of America, and so presumably this could form the basis of an NCND response there as well. New Zealand also recognises the non-disclosure of trade secrets, or other commercially sensitive information, as a basis for an NCND response. This is also the subject of an exemption in the American access to information legislation. Uniquely, New Zealand provides for an NCND response where disclosure would seriously damage

the economy of New Zealand, by prematurely revealing decisions to change or continue Government economic or financial policies.

In Most Jurisdictions, 'Neither Confirm Nor Deny' Arguments are Subject to Review and Require Justification

A government NCND response will not be the end of the matter in the majority of jurisdictions surveyed in this research project. That is, it is clear that NCND should generally be reviewable and justified by the individual or institution seeking to rely on the argument. However, a unifying theme across the jurisdictions is a paucity of in-depth discussion by reviewing bodies, such as courts, of the nature of the review they are engaged in.

In the United States of America, if an NCND response is given, it is possible to appeal the ruling within the agency, and then – if necessary – to the Federal District Court. According to *Wolf v CIA* 473 F.3d 370 (DC Cir. 1980), "an agency's justification for invoking a FOIA exemption is sufficient if it appears 'logical' or 'plausible'". This is a deferential standard of review. There are other narrow bases on which an NCND response might be invalidated. An NCND response cannot be maintained if it can be shown that the government has already officially acknowledged the existence of the record in question: see *Afshar v Dep't of State* 702 F.2d 1125, 1130 (D.C. Circ. 1983. Where an agency has acted in bad faith or concealed violations of the law, an NCND response can also be invalidated, however this is very difficult to establish: see *People for the Am. Way Found. v. NSA* 462 F. Supp. 2d 21, 29–31 (D.D.C. 2006). In addition, if there is a public interest in disclosure in exceptional cases, an NCND response can be rejected: see *Congressional News Syndicate v United States Department of Justice* 348 F. Supp..

Aspects of the Australian NCND regime are not reviewable in a court, unlike in other jurisdictions. Under the Freedom of Information Act 1982 (Cth), a court can review an NCND response. However, notably, this legislation does not apply to intelligence agencies. Instead, the responsible Minister dealing with issues under the Intelligence Services Act 2001 (Cth) can prevent or restrict the provision of operationally sensitive information by issuing a certificate that cannot be questioned in any court or tribunal. In the other fields of law in Australia where NCND arises, a more robust approach has been taken. In *Department of Community Services v Jephcott* (2010) 191 FCR 573, the Federal Court of Australia upheld a decision of the Administrative Appeals Tribunal directing that the Department of Health inform the requester, Mrs Jephcott, as to the existence or non-existence of documents that she had requested. The Court found that there was no evidence that Mrs Jephcott would use the confirmation or denial to deduce the identity or existence of a confidential source of information; she was already aware that her sister had provided information to the Department. Similarly, the Queensland Information Commissioner held in *Est v Department of Family Services and Aboriginal & Islander Affairs* [1995] QICmr 20 that an NCND response should be used "only where special circumstances make its use necessary and appropriate".

In Canada, a statutory review and appeals process exists which may be invoked if an NCND response is given. The Federal Court of Appeal in *Ruby v Canada (Solicitor General)* [2000] 3 FCR 589 said that "the particular nature and purpose of the [Privacy] Act and subsection 16(2) indicate that it was a reasonable exercise of discretion to adopt a general policy of never confirming the existence of information in the bank in question." The Court upheld the NCND policy, but justified it only after reviewing the specific content and purpose of the background legislation. This indicates that the legitimacy of an NCND response will need to be reviewed in each case. Although there has been limited judicial comment on the standard of review to be adopted in NCND appeals, a reasonableness standard appears to be deployed: see *Ruby v Canada (Solicitor General)*. In addition to judicial oversight of NCND use provided by the statutory review and appeals process, there is also a statutory requirement for government institutions to submit reports to parliament detailing the frequency of NCND responses: see section 72 of the Access to Information Act 1985.

The limited comment available in New Zealand on NCND reveals an analogous approach. The Privacy Commissioner rejected police attempts to use NCND in a case involving a request for surveillance information: *Man Seeks Information from Police (Case Note 202975)* [2010] PrivCmr 19. The Commissioner said that it had not been "satisfied" that a confirmation of surveillance would prevent the police's ability to maintain the law. The lack of evidence from the police was dispositive: "the Police did not provide any evidence," said the Commissioner, "as to why the complainant would be likely to commit offences in the future if he knew that he had not been under surveillance in the past." The fact that the NCND argument was not accepted shows that it is, at least in some circumstances, subject to rigorous review in New Zealand.

Therefore, a survey of the review of NCND responses across jurisdictions demonstrates that while review is possible, the precise basis on which it may be carried out, and the willingness of courts to critique a governmental claim that NCND is required, varies. Even within a jurisdiction, the approach can vary from case to case. Given the informational asymmetry and power imbalance between the government and an individual seeking information, it is right that once concern over the appropriateness of an NCND response has been raised by an individual, the onus is on the government to justify its use. Nevertheless, in all jurisdictions, the level of justification required for invocation of NCND could usefully be clarified. Further, one might question whether sufficient judicial oversight is provided when there is a high degree of judicial deference, such as that seen in the United States of America, or where the judiciary is altogether excluded from reviewing intelligence agency responses, as in Australia. A more promising mode of review seems to be present in Canada, where the courts have been willing to engage in a slightly more rigorous reasonableness review of NCND responses, and have stressed the necessity of compliance with the legislative framework governing its use. Canadian legislation also creates the potential for parliamentary oversight, through the requirement that agencies report their rates of NCND usage.

Research Briefs

In this part we present the product of research into the academic literature, case law, and policy work on 'neither confirm nor deny'. We begin with an overview of the academic literature. The remaining sections address jurisdictions: Canada, the United States of America, Australia, and New Zealand. Areas of inquiry include circumstances under which NCND is invoked, the different concerns that have been raised about NCND, and the justifications for NCND that have been given.

Literature Review

There is very little academic literature focused specifically on the 'neither confirm nor deny' policy ('NCND'), although it is often mentioned in passing in articles relating to freedom of information and government secrecy. Of the specific literature on NCND, the majority focuses on the American context.

This brief summary of the available literature will set out the justifications for NCND, justifications for judicial deference to governmental use of NCND, concerns raised about NCND and, finally, proposals that have been made to ensure NCND use is adequately constrained.

Justifications of the 'Neither Confirm Nor Deny' Policy

The underlying rationale for NCND is that revelation of whether or not the government possesses records can sometimes, in and of itself, reveal protected information. In such cases it is not sufficient to refuse disclosure of the documents themselves; the very existence or nonexistence of the documents must not be disclosed.[1] It is not doubted that the government has, in some cases, a legitimate need to invoke NCND.[2]

For NCND to function, it must be applied consistently to requests for the same kind of information, whether or not the government possesses information in the given case. Otherwise, it would be possible to deduce from an NCND response that documentation exists. This systematic application of NCND to certain kinds of information is particularly necessary in the national security context. 'Mosaic theory' 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.[3]

---

[1] Nathan Freed Wessler, '(We) Can Neither Confirm nor Deny the Existence or Nonexistence of Records Responsive to Your Request: Reforming the Glomar Response under FOIA' (2010) 85 New York University Law Review 1381.

[2] ibid; Every American appellate court that has considered the issue agrees that NCND is appropriate in the national security context: Michael D Becker, 'Piercing GLOMAR: Using the Freedom of Information Act and the Official Acknowledgment Doctrine to Keep Government Secrecy in Check' (2012) 64 Administrative Law Review 673.

[3] ibid.

Justifications for Judicial Deference to Governmental Use of the 'Neither Confirm Nor Deny' Policy:

In America there has been routine judicial deference to the use of the Glomar response by government agencies. This deference is often justified on the basis that it is neither constitutionally appropriate, nor feasible, for the courts to provide rigorous oversight.

The argument based on constitutional appropriateness is that in the American context the protection of national security has been entrusted to the executive under the Constitution. Therefore, at least in relation to the deployment of NCND in the national security context, it is not the place of the courts to intervene. However, Wessler roundly rejects this, noting that the American Freedom of Information Act, 5 U.S.C. § 552 ('FOIA') itself mandates a significant role for the courts in reviewing exemptions from disclosure, including those pertaining to national security. He further notes that there is a real interest in judicial oversight, due to the conflict of interest inherent in government agencies making unreviewed decisions to withhold information that those agencies themselves may have a potentially illegitimate interest in keeping secret.[4]

The second argument for judicial deference is that courts are ill-equipped to review the judgments of government agencies when it comes to national security. In the context of a challenge to a NCND response, the reviewing court will have limited information available to it: generally, it must rely upon the representations of the government agency in question. In addition, where NCND is deployed agencies will likely be arguing that the danger of disclosure is acute. Therefore, in the NCND context, judges' fears about mistakenly forcing disclosures that could result in severe harm will be intense. This is further exacerbated by mosaic theory, which suggests that even apparently innocuous disclosures could, in the grand scheme of things, cause serious harm.

Wessler again roundly rejects this rationale for judicial deference. Although he acknowledges the unique position of government agencies in assessing the likely risks of disclosure, Wessler notes that courts frequently do deal with sensitive national security information in other contexts, without grave harm resulting. Furthermore, as mentioned above, the FOIA itself explicitly carves out a role for the courts in assessing government decisions to withhold information, including on the ground of national security.[5] Nevertheless, even if the role of the courts in this domain is recognised, they will remain to a large extent at the mercy of the government, in that they will rely upon government agencies to disclose the information necessary for them to carry out an adequate review. This difficulty can only be overcome if government agencies have sufficient incentive to disclose by, for example, imposing a burden upon them to justify the use of NCND that cannot be discharged without evidence of sufficient quality. Furthermore, government disclosures may only be forthcoming if they can be made within closed proceedings. This

[4] Wessler (n 1).
[5] ibid.

would represent a trade-off between the needs of state secrecy and the interests of open justice.

Academic Concerns About the 'Neither Confirm Nor Deny' Policy

While it is not contested that NCND is a necessary response in some circumstances, the overuse of NCND has been widely criticised.[6] What began as a rarely used response in the 1970s has, since 9/11, become an increasingly common, perhaps even routine, response.[7]

In pursuit of consistency, agencies have used NCND in response to requests for information about completely implausible government activities or operations, that could easily have been denied without harming national security. Similarly, agencies have issued NCND responses to requests for information relating to programs which are already generally known about, where the requestor has good reason to believe the records exist. Becker notes particularly that the practice of issuing a NCND response while simultaneously leaking information to the press, such as occurred in relation to America's covert drone program, not only undermines the spirit of the FOIA but may also undermine the rule of law.[8] More problematic still is the use of NCND by agencies to conceal illegal or embarrassing conduct, particularly where there is already information in the public domain casting doubt on the legality of government conduct. All these forms of overuse undermine government credibility and the public's trust in legitimate secrecy.[9]

At present, the NCND response presents grave difficulties for both those requesting information, and for courts reviewing NCND responses. An NCND response starves both a requestor and a reviewing court of the information necessary to effectively challenge or review an agency's decision to issue an NCND response.[10] Currently, in NCND cases courts can require government agencies to prepare public affidavits, describing in as much detail as possible the logical basis for their response. This is provided for in *Phillippi v CIA*, 546 F.2d 1009. However, *Phillippi* affidavits have in practice become increasingly boilerplate, providing limited insight into agency reasoning.[11] Furthermore, because of the sensitive nature of information supposedly at stake, a public affidavit cannot provide the detailed information a court needs to meaningfully review an agency's decision.[12] Public affidavits can be supplemented by the submission of classified declarations to the court, to be considered *in camera* and *ex parte*.

---

[6] See ibid; Joshua R Chazen, 'Electronic Privacy Information Center v National Security Agency: How Glomar Responses Benefit Businesses and Provide an Epic Blow to Individuals' (2014) 9 Journal of Business and Technology Law 315; Becker (n 3); See: John Y Gotanda, 'Glomar Denials under FOIA: A Problematic Privilege and a Proposed Alternative Procedure of Review' (1994) 56 University of Pittsburgh Law Review 186; Wessler (n 1).
[7] Becker (n 3).
[8] ibid.
[9] Wessler (n 1); Becker (n 3).
[10] Wessler (n 1); Gotanda (n 7); Chazen (n 7).
[11] Becker (n 3).
[12] Gotanda (n 7).

However, this too may prove inadequate, depending on the level of disclosure made by the agency. The government agency, in controlling the information disclosed, effectively controls judicial proceedings.[13] Even if useful information is disclosed to the court during the *in camera* review, the requestor is not present to identify specific issues that may arise, and the public record of the decision will be undermined.[14] Therefore, at present, requestors and courts have extreme difficulty assessing the propriety of a government agency's NCND response, which means it can readily be abused.[15]

Proposals for Greater Oversight of the 'Neither Confirm Nor Deny' Policy

Academic proposals for oversight of the use of NCND extend beyond strengthening judicial review, to include possible executive and legislative action.

Judicial Oversight

Wessler argues that judicial scrutiny should be made more robust in the following ways: first, the judiciary should apply the existing bad faith standard: more aggressively that is, that a requestor can force disclosure of the existence or nonexistence of requested records if they can show that the government is acting in bad faith or concealing violations of the law. The judiciary should insist on specific, not boilerplate, justifications to be given, and should probe agencies to determine the true necessity of the NCND response. Second, the judiciary should take advantage of *in camera* reviews to demand from agencies more evidence to justify their response, including any underlying records (if they exist) or an admission that records do not exist if that is the case.[16]

Similarly, Becker argues that the judiciary should interpret and apply the official acknowledgement doctrine more broadly: that is, that a requestor can force disclosure of the existence or nonexistence of requested records if they can show that the government has already officially acknowledged the existence of the records. Currently, the official acknowledgement doctrine is very narrowly applied. Becker argues that, for the doctrine to apply, it should be sufficient to show a disclosure by any official in a position to know of what he spoke, no matter how inconvenient or inadvertent this disclosure. Similarly, he argues that agencies should be precluded from relying on an NCND response in circumstances where the requested information has been purposefully placed in the public domain, for example, through strategic, anonymous leaks.[17]

Legislative Reform

A number of legislative reforms have been proposed by academics:

[13] Aitchison (n 6).
[14] Gotanda (n 7); Becker (n 3).
[15] Aitchison (n 6).
[16] Wessler (n 1); Although, Gotanda objects to this on the basis that it would draw courts into a sham review, if no documents exist. See: Gotanda (n 7).
[17] Becker (n 3).

a. It should be stated in legislation that NCND is to be used only as a last resort.[18]
b. Legislation should provide for reporting requirements on NCND usage, which will help reveal agency practices and improve oversight.[19]
c. Legislation should set out clearly when NCND cannot be used, for example, by codifying the bad faith and official acknowledgement doctrines.[20]
d. Legislation should confer on courts the power to coerce compliance from agencies who fail to provide adequate affidavits. Specifically, the courts should have the power to order live testimony from agency officials, which would allow for judicial questioning and further information to be gathered.[21]

Executive Actions

Wessler argues that regulation of agency use of NCND can be improved at the level of individual agencies and across the entire executive branch:

- All agencies should publish rules governing the use of NCND. These rules should make it clear that it is never appropriate to use NCND to conceal agency wrongdoing or avoid embarrassment. It should also be made clear that NCND should only be used as a last resort, when no other response will protect legitimately classified information.
- In America, the Attorney-General sets out broad priorities for FOIA implementation through a memoranda circulated to government departments and agencies. Included in this memorandum are details of the standards the Department of Justice will use in deciding whether to defend an agency's withholding decision in court. The Attorney-General should draft and circulate standards specific to NCND, making it clear that the Department of Justice will only defend an agency's use of NCND if its use is required to avoid serious and foreseeable harm to national security (or on the basis of another qualifying ground), and where no other response will suffice.
- There should be a legislatively created body empowered to oversee agency compliance with the FOIA generally. This body should oversee the use of NCND, tracking rates of usage and drafting best practice guidelines. [22]

[18] Wessler (n 1); Aitchison (n 6).
[19] Wessler (n 1).
[20] ibid; Becker (n 3).
[21] Aitchison (n 6).
[22] Wessler (n 1).

Canada

Public Discourse Concerning NCND

The federal Canadian government uses NCND responses. Canadian privacy and access to information legislation – Privacy Act 1985 and Access to Information Act 1985[23] – enables the government to respond to requests for access to information with an NCND response.

Briefly, any federal government institution that responds to access to information and disclosure requests can use an NCND response.[24] Government institutions also have to submit reports to Parliament, under section 72 of the Access to Information Act, detailing the frequency of NCND responses. For example, the department of Citizen and Immigration Canada, in their 2014-2015 Access to Information and Privacy Report, stated that for 7 of the total 34,066 Access to Information requests received they answered that, "either no records existed, request was transferred, request abandoned or request was neither confirmed nor denied."[25]

In general, a government body can use the NCND response if the request relates "[to] the detecting, preventing or suppressing subversive or hostile activities."[26] Reported instances of receiving an NCND response to an access to information request have been in relation to questions regarding surveillance or monitoring.[27]

While this report does not consider the Access to Information regime in detail, it is worth noting that a statutory review and appeals process exists for individuals to appeal an NCND response to an Access to Information request. An example of this was the "stingray" controversy.

An Access to Information Request was made to the Toronto Services Policy Board, requesting the records of any stingray purchases; stingrays are an International Mobile Subscriber Identity, a type of high-tech surveillance equipment that enables police to survey mobile conversations and text messages.[28] In response to this request, the Toronto Services Police Board responded:

---

[23] *Privacy Act,* RSC, 1985, c. P-21; *Access to Information Act*, RSC, 1985, C. A-1.
[24] There is also corresponding provincial legislation.
[25] Citizenship and Immigration Canada Government of Canada, 'Access to Information Act, Privacy Act' (2015) <http://www.cic.gc.ca/english/resources/publications/privacy/atip2014-15.asp> accessed 4 December 2015.
[26] Carol Linnitt, 'CSIS "Can Neither Confirm Nor Deny" Spying on Me (Or You For That Matter)' <http://www.desmog.ca/2015/03/03/csis-can-neither-confirm-nor-deny-spying-me-or-you-matter> accessed 4 December 2015.
[27] ibid; Justin Ling, '"No Comment": Ferreting out Information from CSIS' <http://www.cjfe.org/_no_comment_ferreting_out_information_from_csis> accessed 4 December 2015.
[28] Robin Levinson King, 'Canada's Two Largest Police Forces Are Refusing to Say If They Use Stingrays, Which Work by Scooping up the Cellphone Signals of Everyone Nearby.' *The Toronto*

> ". . . [D]ue to the nature of your inquiry surrounding the use of electronic surveillance devices, disclosing such information could reveal classified operational procedures currently in practice by the Police Service; thus, potentially jeopardizing the effectiveness in fulfilling its policing mandate."

This response was appealed to the Office of the Ontario Privacy Commissioner, in accordance with review and appeal procedures. Adjudicator Donald Hale found that, "the disclosure of this information respecting the existence or non-existence of responsive records could reasonably be expected to reveal investigative techniques which are either in use or could likely be used in law enforcement," upholding the Police Board's decision.[29]

In public discourse, and outside of the request to information, we were only able to find a few examples of NCND reported in the recent media.[30] These examples, however, span different subject matter areas.

For instance, one widely documented instance where an NCND response was used politically was in relation to foreign intelligence activities. In 2013, some of the documents leaked by Edward Snowden revealed Canada's cryptology agency, the Communities Security Establishment Canada (CSEC),[31] along with the United States, had been surveying oil and gas companies in Brazil to perform "economic espionage."[32] In response to these allegations, the Prime Minister's spokesperson said he would "neither confirm or deny the allegations." Similarly, in response to this incident, the Prime Minister's communications director Jason MacDonald stated that "CSEC does not comment on its specific foreign intelligence activities or capabilities."[33]

This response has also been used in the face of domestic issues that relate to foreign activities. For example, in 2012 there were rumours circulating of significant federal budget cuts. When asked if the Foreign Affairs department would experience budget

---

Star (15 December 2015) <http://www.thestar.com/news/canada/2015/12/15/the-cellphone-spyware-the-police-dont-want-to-acknowledge.html> accessed 16 December 2015.

[29] Donald Hale, Order MO-3236, Appeal MA14-412 2015.

[30] This was done by a search of online Canadian media – not an extensive search into archived media reports and newspapers.

[31] Now known as the Communications Security Establishment.

[32] Jon Queally, 'Spying for Economic Gain: Canada's CSEC Targeted Brazilian Energy Firms' <http://www.commondreams.org/news/2013/10/07/spying-economic-gain-canadas-csec-targeted-brazilian-energy-firms> accessed 12 December 2015; Isabel Teotonio, 'Brazil Demands Explanation over Reports Canada Spied on Mine Ministry' *The Toronto Star* (7 October 2013) <http://www.thestar.com/news/world/2013/10/07/canada_spied_on_brazils_mines_and_energy_ministry_report.html> accessed 11 December 2015.

[33] Queally (n 10); Teotonio (n 10).

cuts, the Foreign Affairs department would "neither confirm nor deny the cuts" as "the department did not want its employees learning their fate in the media."[34]

An NCND response has also been used politically in answering questions regarding potential election fraud. The Council for Canadians, an independent national government watchdog organization, publicly asserted that the Commissioner of Canada Elections should re-open an investigation into an alleged case of election fraud in 2011. In response the Elections Commissioner said his office "can neither confirm nor deny whether the investigation will continue."[35]

There do not seem to be significant instances in recent history of the Canadian government using an NCND response in relation to a highly controversial issue. Nevertheless, it appears the media and news industry have become accustomed to receiving NCND responses, especially in relation to surveillance, monitoring, and the activities of the intelligence agencies.

2. Accountability Bodies' Discussion of 'Neither Confirm Nor Deny'

As outlined in the previous section, Canada has a system to request reviews, and appeal responses to access to information requests. This allows tribunals and courts to ensure NCND responses are being used legitimately. As governmental bodies also have to report the use of NCNDs, there is a system for accountability in place within the government. Furthermore, government departments and institutions may have their own ombudsman or watchdog that may consider NCND issues in the context of their institutions. Outside of these government mechanisms, however, it appears there is a limited pool of accountability bodies interested in NCND responses in Canada.

We could not find any body that was specifically responsible for NCND responses. The Office of the Privacy Commissioner of Canada's mandate includes overseeing compliance with Privacy Act 1985, "which covers the personal information-handling practices of federal government departments."[36] While this would include overseeing NCND responses given to individuals under the Privacy Act, it does not specifically review the actions of the Canadian government or intelligence agencies, nor does it appear to have a specific interest in exploring NCND responses in their own right.

Previously, Canada has had an Inspector General ("IG") of the Canadian Security Intelligence Service ("CSIS"). The IG was the Minister of Public Safety's watchdog for

---

[34] Greg Weston, 'Foreign Affairs Prepares to Cut, Diplomatically' *CBC News* (27 April 2012) <http://www.cbc.ca/news/politics/foreign-affairs-prepares-to-cut-diplomatically-1.1173809> accessed 11 December 2015.

[35] Council for Canadians, 'Del Mastro Found Guilty of Election Fraud but Pierre Poutine Still at Large' <http://canadians.org/media/del-mastro-found-guilty-election-fraud-pierre-poutine-still-large> accessed 12 December 2015.

[36] Government of Canada, 'Mandate and Mission' (*Office of the Privacy Commissioner of Canada*) <www.priv.gc.ca/au-ans/mm_e.asp>.

CSIS, and would provide an annual certificate declaring whether CSIS had acted outside the law or exercised its powers unreasonably – and who may have taken up this issue.[37] Former Prime Minister, Stephen Harper, eliminated this position in 2012.[38] The IG's functions were said to be replaced by the Security Intelligence Review Committee (SIRC), a panel made of part-time employees who review CSIS' activities after-the-fact. The SIRC's role has been described as significantly different from the IG, and at the time the last IG, Eva Plunkett, retired, Canadian news outlets stated the SIRC appeared unable to adequately carry-on the IG's former watchdog function.[39]

Additionally, we surveyed the publications of the following external third-party national government watchdogs: Council for Canadians,[40] Democracy Watch,[41] Canadian Civil Liberties Association,[42] Canadians for Accountability,[43] and National Citizens Coalition.[44] While all these organizations were concerned, to varying degrees, with issues of transparency, surveillance and monitoring, none appeared specifically concerned with NCND responses.

Based on this preliminary review, we cannot find an accountability body in Canada that has engaged in an in-depth discussion of NCND responses.

Judicial Treatment of 'Neither Confirm Nor Deny'

There is a significant number of tribunal and court decisions concerning NCND responses in the context of administrative reviews from access to information requests, both federally and provincially.[45]

---

[37] Centre for International Policy Studies, University Of Ottawa, 'CSIS Inspector General Certificate Reports' (*Centre for International Policy Studies*) <www.cips-cepi.ca/publication/thematic-series/csis_certificate_archive/>.

[38] 'Axing CSIS Watchdog "Huge Loss," Says Former Inspector General' *CBC News* (10 August 2012) <http://www.cbc.ca/news/politics/axing-csis-watchdog-huge-loss-says-former-inspector-general-1.1143212> accessed 11 December 2015.

[39] Carol Linnitt, 'How Come CSIS "Can Neither Confirm Nor Deny" Spying On Me?' *The Huffington Post* <http://www.huffingtonpost.ca/carol-linnitt/government-spying_b_6794186.html> accessed 19 December 2015; 'Axing CSIS Watchdog "Huge Loss," Says Former Inspector General' (n 16).

[40] 'The Council for Canadians' (*The Council for Canadians*) <http://canadians.org/>.

[41] 'Democracy Watch' (*Democracy Watch*) <http://democracywatch.ca/>.

[42] 'Canadian Civil Liberties Association' (*Canadian Civil Liberties Association*) <https://ccla.org/>.

[43] 'Canadians for Accountability' (*Canadians for Accountability*) <http://canadians4accountability.org>.

[44] 'National Citizens Coalition' (*National Citizens Coalition*) <https://nationalcitizens.ca/>.

[45] Such as: *Saskatchewan Workers' Compensation Board (Re)*, 2013 CanLII 69841 (SK IPC), <http://canlii.ca/t/g1qg9>; *The Board of School Trustees of School District No. 68 (Nanaimo-Ladysmith)*, 2004 CanLII 34258 (BC IPC), <http://canlii.ca/t/1ggpf>; *Ontario (Natural Resources) (Re)*, 1991 CanLII 4057 (ON IPC), <http://canlii.ca/t/1rlcz>; *Law Society of British Columbia (Re)*, 2008 CanLII 65714 (BC IPC), <http://canlii.ca/t/21w34>; *University of British Columbia, Re*, 1998 CanLII 3617 (BC IPC), <http://canlii.ca/t/1gdnt>.

In terms of judicial treatment of NCND responses, the leading case is *Ruby v Canada (Solicitor General)*.[46] In *Ruby*, an individual made a request for personal information held in information banks maintained by CSIS, the Royal Canadian Mounted Police (RCMP), and the Department of Foreign Affairs and International Trade (DEA). The DEA and CSIS refused to confirm or deny the existence of the information requested, and held if it did exist it would have been exempt from disclosure under the relevant provisions of the federal Privacy Act. In this case the Federal Court of Appeal confirmed the government institution's right under subsection 16(2) of the Privacy Act to adopt a blanket policy of providing NCND responses to request for personal information that existed within certain information banks:

> "[T]he particular nature and purpose of the [Privacy] Act and subsection 16(2) indicate that it was a reasonable exercise of discretion to adopt a general policy of never confirming the existence of information in the bank in question. Elsewhere in the Act, the government has been given a wide scope for protecting secrecy of law enforcement related banks where secrecy is deemed appropriate. By providing the option under subsection 16(2) of refusing to confirm or deny the existence of personal information, Parliament offered one more such mechanism, allowing government institutions the possibility of maintaining not just the content but also the existence of records confidential. In the cat-and-mouse games that spies and criminals play with law enforcement agencies, for the agency to feel bound to reveal information in certain circumstances could create opportunities for educated guesses as to the contents of information banks based on a pattern of responses. To adopt a generalized policy of always refusing to confirm the existence of personal information eliminates this threat."[47]

Thus, while the Court confirmed that a government institution can adopt a blanket policy of NCND responses for requests of information held in certain information banks, a Court can still review the reasonableness of that decision.

Ruby was upheld in *Westerhaug v. Canadian Security Intelligence Service*:[48]

> "The Federal Court of Appeal in *Ruby* held that adopting a policy of non-disclosure was reasonable given the nature of the information bank in question, because merely revealing whether or not the institution had information on an individual would disclose to him whether or not he was a subject of investigation. I agree. If it is in the national interest not

---

[46] *Ruby v. Canada (Solicitor General)*, [2000] 3 FCR 589, 2000 CanLII 17145 (FCA), <http://canlii.ca/t/4l09>.

[47] *Ruby v Canada*, (n 24), para 66 (emphasis added).

[48] *Westerhaug v. Canadian Security Intelligence Service*, 2009 FC 321 (CanLII), <http://canlii.ca/t/233l7>.

> to provide information to persons who are the subject of an investigation, then it follows that it is also in the national interest not to advise them that they are or are not the target of an investigation. It is one of the unfortunate consequences of adopting such a blanket policy that persons who are not the subject of an investigation and who have nothing to fear from the government institution will never know that they are not the subject of an investigation."[49]

More recently, *Ruby* was applied in *Braunschweig v. Canada (Public Safety)*.[50]

Canadian courts have also considered the constitutionality of NCND responses, in, for example, the seminal case of *Zanganeh v Canada Security Intelligence Service* (cited by *Ruby*).[51] In *Zanganeh*, the Court held that NCND responses, when given in accordance with the relevant provisions of the Privacy Act, were constitutional under the Canadian Charter of Rights and Freedoms:

> "In light of six years of rhetoric and jurisprudence about the Charter, some Canadians may shudder to realize that the security needs of a free and democratic society are, in a few basic essentials, much the same as those which totalitarian societies arrogate unto themselves. Utter secrecy, subject to certain checks, in security intelligence matters is one. That necessary degree of secrecy is so much more fissiparous in freedom and democracy than it is under the stifling oppression of a totalitarian regime, and it is therefore objectively justifiable in terms of paragraph 46(1)(*b*) of the *Privacy Act*. What no doubt distinguishes this free and democratic society from those which are less or not at all so, are the right to apply for, and obtain the results of, the Privacy Commissioner's investigation, and the right to apply to this Court for a review.
>
> ....
>
> When, however, as here, the respondent's conduct is lawfully in conformity with the *Privacy Act* and with its own statute, the tight secrecy of its information, if any, including the secrecy of whether it even has any information is justified not only under that ordinary legislation but, more importantly, justified under section 1 of the Charter."[52]

---

[49] *Westerhaug*, (n 26), para 18.
[50] *Braunschweig v. Canada (Public Safety)*, 2014 FC 218 (CanLII), <http://canlii.ca/t/g670n> at [45].
[51] *Zanganeh v Canadian Security Intelligence Service*, [1989] 1 FC 224, 50 DLR (4th) 747.
[52] *Zanganeh*, (n 29), para 12 & 14.

Summary

(i) When (in relation to what subject matters) and by whom is NCND commonly deployed?

The Canadian federal government uses NCND responses, most commonly in response to requests for information under various legislative schemes. Provincial governments, with similar legislation, also use NCND responses. The Canadian government has issued NCND responses in relation to a wide range of subject matter.

(ii) What concerns have been raised over the use of NCND, if any, and by whom?

The Canadian media has raised concerns over the use of NCND. It does not appear to be, at least in recent media, a highly contested issue in Canada.

(iii) What controls or oversight, if any, is there of the use of NCND policy? Or, what controls or oversight have been recommended, and by whom?

Canada has a system to request reviews, and appeal responses to access to information requests. This allows tribunals and courts to ensure NCND responses are being used legitimately. As governmental bodies also have to report the use of NCNDs, there is a system for accountability in place within the government. Furthermore, government departments and institutions may have their own ombudsman or watchdog that may consider NCND issues in the context of their institutions. We could not find a governmental body or institution specifically concerned with NCND responses.

The United States of America

Standard Freedom of Information Act Procedure

First enacted in 1966, the Freedom of Information Act (FOIA) is a federal law that provides that a person has a general right to obtain access to federal agency records upon making a request. The FOIA applies only to federal agencies. Under normal FOIA procedure, one submits a request for records of a government agency, the agency is supposed to search for the records, and the requestor will receive one of three responses:

A) The agency will identify the records asked for and release them;
B) The agency will determine that the records asked for do not exist and will inform the requestor; or
C) The agency will determine that the records requested are exempted from disclosure under the Freedom of Information Act.

The FOIA contains nine statutory exemptions:

1. Those documents properly classified as secret in the interest of national defense or foreign policy;[53]
2. Related solely to internal personnel rules and practices;[54]
3. Specifically exempted by other statutes;[55]
4. A trade secret or privileged or confidential commercial or financial information obtained from a person;[56]
5. A privileged inter-agency or intra-agency memorandum or letter;[57]
6. A personnel, medical, or similar file the release of which would constitute a clearly unwarranted invasion of personal privacy;[58]
7. Compiled for law enforcement purposes, the release of which
    a. could reasonably be expected to interfere with law enforcement proceedings,
    b. would deprive a person of a right to a fair trial or an impartial adjudication,
    c. could reasonably be expected to constitute an unwarranted invasion of personal privacy,
    d. could reasonably be expected to disclose the identity of a confidential source,
    e. would disclose techniques, procedures, or guidelines for investigations or prosecutions, or

[53] §552(b)(1)
[54] §552(b)(2)
[55] §552(b)(3)
[56] §552(b)(4)
[57] §552(b)(5)
[58] §552(b)(6)

f. could reasonably be expected to endanger an individual's life or physical safety;[59]

8. Contained in or related to examination, operating, or condition reports about financial institutions that the SEC regulates or supervises;[60] or
9. Documents containing exempt information about gas or oil wells.[61]

The Courts have said that these statutory exemptions must be construed narrowly, with a presumption in favour of disclosure.[62] If an agency denies a request under the FOIA exemptions, the requestor may file an appeal within the agency[63] and if the agency upholds the denial on the appeal then the requestor can bring suit in a federal district court.[64] Once the case goes to court the court will review the agency decision and will examine the documents *in camera* to determine whether they meet the criteria for non-disclosure under the FOIA exemptions. The agency will then provide the requestor with an affidavit, called a Vaughn Index,[65] which discharges the agency's burden of proof by describing the contents of the withheld document(s) in enough detail to provide a basis for contesting the withholding. Although there is a presumption in favour of disclosure when the agency's records are based on national security concerns the court "must accord substantial weight to the Agency's determinations".[66]

The Creation of the "Glomar response"

In addition to the three statutory responses to a FOIA request, a fourth non-statutory response has developed, where agencies "neither confirm nor deny" whether responsive records exist, which is referred to as a 'Glomar response'. The name comes from the first judicial recognition of "neither confirm nor deny" in *Phillippi v CIA*[67] and *Military Audit Project v Casey,*[68] two cases which involved a ship named the Hughes Glomar Explorer. In 1968 a Soviet submarine called K-129 carrying nuclear missiles sank in the North Pacific Ocean. While the Soviets were unable to locate their submarine, the US Navy found it but could not access it because it was more than 3 miles deep. The project was turned over to the CIA, who endeavoured to retrieve the ship so as to study the sunken Soviet missiles. While the CIA was able to contract for the building of an enormous submersible barge for the recovery mission, the CIA needed a cover story for why the barge was in the area that the submarine was known to have sunk lest the USSR notice

---

[59] §552(b)(7)
[60] §552(b)(8)
[61] §552(b)(9)
[62] *Vaughn v Rosen* 484 F.2d 820, 823 (D.C. Cir. 1973) "This court has repeatedly stated that these exemptions from disclosure must be construed narrowly, in such a way as to provide the maximum access consonant with the overall purpose of the Act."
[63] § 552(a)(6)(A)
[64] § 552(a)(4)(B).
[65] See *Vaughn* at 826-828
[66] *Gardels v. CIA*, 689 F.2d 1100, 1104 (D.C. Cir. 1982) (internal quotation marks omitted) (citing *Ray v. Turner*, 587 F.2d 1187, 1194 (D.C. Cir. 1978))
[67] *Phillippi I*, 546 F.2d at 1009
[68] 656 F.2d 724 (D.C. Cir. 1981).

and interfere. The CIA enlisted the help of eccentric billionaire business tycoon Howard Hughes to put his name to the project and say that the ship, the "Hughes Glomar Explorer" was mining manganese nodules from the ocean floor. The Los Angeles Times broke part of the story in 1975 which prompted the CIA to bury the story. A journalist for the LA Times, Harriet Phillippi, filed a FOIA request with the CIA for all information on the Glomar explorer and the attempts to bury the story. Concurrently, Military Audit Project made a similar FOIA request. To that point, the CIA would have given the third response, that the records exist but are exempt due to national security, either under Exemption 1 or 3 of the FOIA. However, to do that would mean that there were records of the CIA financing this particular project, which was the essence of the claim. Therefore, the (C) response would be tantamount to an acceptance. The CIA stated that "the fact of existence or nonexistence of the records" requested was exempt from disclosure as a matter of national security.[69] The court held that this was permissible under the FOIA.

It is interesting to note that this has been a judicial development, and one that Congress has chosen not to amend the FOIA to cover. In *Public Citizen v Department of State*[70] Edwards J holds that:

> "[C]ontentions that it is unfair, or not in keeping with FOIA's intent, to permit State to make self-serving partial disclosures of classified information are properly addressed to Congress, not to this court […] If the legislature believes that this outcome constitutes an abuse of the agency's power to withhold documents under exemption 1, it can so indicate by amending FOIA."[71]

However, in the context of national security, the Glomar response is embedded in US Code Title 50 §435 Sec. 3.6(a):

> "An agency may refuse to confirm or deny the existence or nonexistence of requested records whenever the fact of their existence or nonexistence is itself classified under this order or its predecessors."

How the Glomar Response Works

As confirmed in *Wilner v NSA*:

> "To properly employ the Glomar response to a FOIA request, an agency must 'tether' its refusal to respond to one of the nine FOIA exemptions—in other words, 'a government agency may ... refuse to confirm or deny the existence of

[69] *Phillippi* at 1011-12

[70] 11 F.3d 198, 199 (D.C. Cir. 1993)

[71] Ibid at 26

> certain records [...] if the FOIA exemption would itself preclude the acknowledgment of such documents.'"[72]

The Glomar response has been accepted in relation to Exemption 6 and 7(c) concerning "unwarranted invasion of personal privacy" and in relation to Exemption 1 and 3 on the grounds of national security.

The primary difference from response (C) and Glomar is that the FOIA compels non-Glomar cases to create a *Vaughn* index and allow *in camera* review of records whereas in Glomar cases the defendant agency must prepare a public affidavit explaining the justifications for neither confirming or denying the existence of the record.[73] However, because the justification for giving a Glomar response is often based on sensitive and classified material, it is common for agencies to not give a public affidavit to the plaintiffs but instead to submit classified declarations to the court to be considered *in camera*.[74] The courts "must take into account that any affidavit or other agency statement of threatened harm to national security will always be speculative to some extent, in the sense that it describes a potential future harm."[75] In *Wolf I* it was held that "an agency's justification for invoking a FOIA exemption is sufficient if it appears 'logical' or 'plausible'".[76] Due to this low burden of proof justifying the use of NCND and deference to the agency's assessment, courts tend to accept Glomar responses.[77]

A) Personal Privacy Exemption Under 7(c)

Though the Glomar response was created in a national security context, the response has also been accepted in relation to FOIA exemption 7(c), information which "could reasonably be expected to constitute an unwarranted invasion of personal privacy". Agencies that maintain investigatory files have successfully argued that disclosing that an individual has been the subject of an investigation is stigmatizing and produces "the unwarranted result of placing the named individuals in the position of having to defend their conduct in the public forum outside of the procedural protections normally afforded to the accused in criminal proceedings."[78] In *Baez v Department of Justice*[79] it was held that "[t]here can be no clearer example an unwarranted invasion of personal privacy

---

[72] *Wilner v. NSA*, 592 F.3d 60, 71 (2d Cir. 2009) at 71 quoting from *Minier,* 88 F.3d at 800.

[73] Wilner v NSA 592 F.3d at 60, 68 (2d Cir. 2009)

[74] See *Bassiouni v. CIA*, 392 F.3d 244, 246 (7th Cir. 2004) ("Every appellate court to address the issue has held that the FOIA permits the CIA to make a 'Glomar response' when it fears that inferences from Vaughn indexes or selective disclosure could reveal classified sources or methods of obtaining foreign intelligence.")

[75] *Halperin v CIA*, 629 F.2d 144, 149 (D.C.Cir.1980)

[76] *Wolf v. CIA,* 473 F.3d 370, 374–75 (D.C. Cir. 2007) citing *Gardels*, 689 F.2d at 1105; *Hayden v. NSA*, 608 F.2d 1381, 1388 (D.C.Cir.1979).

[77] See *ACLU*, 389 F. Supp. 2d at 562 ("[T]he courts generally respect the CIA's right to make a Glomar response.")

[78] *Fund for Constitutional Government v National Archives and Records Service* 656 F.2d 856 (D.C. Cir. 1981) [at 865]

[79] 647 F.2d 1328 (D.C. Cir. 1980) [at 1338]

than to release to the public that another individual was the subject of a FBI investigation."

A Glomar response tethered to the 7(c) exemption does not apply in three cases where the privacy interest does not exist. First, deceased people have no protectable privacy interests under the FOIA and so Glomar denials tied to exemption 7(c) may not be invoked.[80] Second, if the third-party subject of a request has provided the requestor with a written waiver of their privacy rights, privacy exemptions cannot be invoked.[81] Third, the exemption will not apply if the federal government has officially confirmed that the third party was the subject of a federal investigation.[82] This is similar to the 'doctrine of official acknowledgment' that invalidates Glomar responses in the context of national security.

B) National Security Exemptions Under 1 and 3

Exemption 1 protects information that has been classified "under criteria established by an Executive Order to be kept secret in the interest of national defense or foreign policy".

Executive Order 13526, signed by President Obama in 2009, lists in Sec. 1.4:

(a) military plans, weapons systems, or operations
(b) foreign government information;
(c) intelligence activities (including covert action), intelligence sources or methods, or cryptology;
(d) foreign relations or foreign activities of the United States, including confidential sources;
(e) scientific, technological, or economic matters relating to the national security;
(f) United States Government programs for safeguarding nuclear materials or facilities;
(g) vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans, or protection services relating to the national security; or
(h) the development, production, or use of weapons of mass destruction.

Exemption 3 protects information that is prohibited from disclosure by other statutes. Exemption 3 is often tied to the National Security Act 1947[83] which requires that the CIA director protect sources and methods,[84] and to the National Security Act of 1959

[80] *Tigar & Buffone v United States Department of Justice*, Civil No. 80-2382, slip op at 9-10 (D.D.C. 1983); *Diamond v FBI*, 532 F. Supp. 216, 227 (S.D.N.Y. 1981)
[81] http://www.justice.gov/oip/blog/foia-update-oip-guidance-privacy-glomarization
[82] *Heimerle v United States Department of Justice* Civil No. 83-1944-(MEL) slip op. at 5 (S.D.N.Y 1985)
[83] Nat'l Sec. Act of 1947, Pub. L. No. 80-253, 61 Stat. 495 (codified at 50 U.S.C. §401 (2006)).
[84] Ibid s102(d)(3)

which exempts information regarding the activities of the National Security Agency.[85] Many other statutes have also been found to qualify under Exemption 3.[86] In these cases courts determine whether acknowledging the existence or non-existence reveals information protected by the statute that is providing grounds for the proposed exemption.

Invalidating a Glomar Response

A) Doctrine of Official Acknowledgment

A requestor can seek to invalidate a Glomar response by proving that the government has already "officially acknowledged" the existence of the record,[87] known as the doctrine of official acknowledgment. It is accepted that Federal agencies may waive their right to a FOIA exemption that would otherwise be valid if the information is in the public domain because "publicly known information cannot be withheld under exemptions 1 and 3".[88] The D.C. Circuit Court, which sees the majority of FOIA litigation[89] has developed a three-part test for determining whether information has or has not been officially acknowledged.

> "First, the information requested must be as specific as the information previously released. Second, the information requested must match the information previously disclosed; we noted, for example, that official disclosure did not waive the protection to be accorded information that pertained to a later time period. Third, we held that the information requested must already have been made public through an official and documented disclosure."[90]

This test is extremely difficult to satisfy. The third criterion in particular, has proved to be a roadblock for requestors who attempt to use an official disclosure about an agency programme by another agency.[91] For instance, in *Frugone v CIA*,[92] Frugone claimed to be employed by the CIA but when he asked for documents related to his employment to contest an issue with his pension the CIA gave a Glomar response to whether or not they had any information about him. Frugone pursued a FOIA claim but the agency tethered their Glomar response to Exemptions 1 and 3. The appeal concerned Frugone contending that his employment had been officially acknowledged by the Office of

---

[85] § 6

[86] For a full list see Office of Information Policy, "Statutes Found to Qualify Under Exemption 3 of the FOIA" US Department of Justice, Dec. 2015 http://www.justice.gov/oip/page/file/623931/download

[87] *Fitzgibbon v. CIA*, 911 F.2d 755, 765 (D.C. Cir. 1990)

[88] *Afshar v Dep't of State*, 702 F.2d 1125, 1130 (D.C. Circ. 1983)

[89] Becker, "Piercing *Glomar*: Using the Freedom of Information Act and the Official Acknowledgment Doctrine to Keep Government Secrecy in Check" (2012) Admin Law Review p. 683

[90] *Afshar* at 702, affirmed in Fitzgibbon at 44

[91] Hunt v. CIA, 981 F.2d 1116, 1120 (9th Cir. 1992)

[92] *Frugone v. CIA*, 169 F.3d 772, 774 (D.C. Cir. 1999)

Personnel Management (OPM) sending him a series of letters which confirmed his status as a former employee of the CIA. He argued that because the OPM was a branch of the Executive they could bind the CIA. This argument failed. Ginsburg J's judgment responded directly, holding that "[i]f Frugone were right, however, then other agencies of the Executive Branch--including those with no duties related to national security--could obligate agencies with responsibility in that sphere to reveal classified information."[93]

In 2007, author Paul Wolf won a rare victory against a Glomar response on the grounds of official acknowledgement. Wolf sought all CIA records related to Jorge Elicécer Caitàn, a Colombian Populist presidential candidate, assassinated in 1948. Here, Wolf successfully argued that the CIA could not use a Glomar response to his request because the director of the CIA had acknowledged the existence of the records during a congressional hearing the year of the assassination.

Concerning the torture and rendition programme, it is clear that the CIA was selectively leaking information to journalists but ensuring that the person giving the information could not be attributed to a member of the CIA so they would not have to disclose under the official acknowledgment doctrine. The Senate Select Committee on Intelligence's Report on the CIA Torture and Interrogation Progamme contains this passage:

> "After the April 15, 2005 National Security Principals Committee meeting, the CIA drafted an extensive document describing the CIA's Detention and Interrogation Program for an anticipated media campaign. CIA attorneys, discussing aspects of the campaign involving off-the-record disclosures, cautioned against attributing the information to the CIA itself. One senior attorney stated that the proposed press briefing was 'minimally acceptable, but only if not attributed to a CIA official.' The CIA attorney continued: 'This should be attributed to an 'official knowledgeable' about the program (or some similar obfuscation), but should not be attributed to a CIA or intelligence official.'"[94]

Therefore, it is possible for agencies to issue Glomar responses when details are publicly known, but where there has been no official acknowledgment. This occurred in the Glomar explorer cases *Phillippi* and *Military Audit Project*, and in relation to the torture and rendition programme. This approach to NCND has been criticized as an over-use of the response.[95]

B) Doctrine of Bad Faith

---

[93] *Frugone v. CIA*, 169 F.3d 772, 777 (D.C. Cir. 1999)

[94] Senate Select Committee on Intelligence, "Torture Report: Committee Study of Central Intelligence Agency's Detention and Interrogation Programme" p. 404

[95] Wessler, "'[We] Can Neither Confirm Nor Deny the Existence or Nonexistence of the Records Responsive to Your Request': Reforming the Glomar Response Under FOIA" (2010) NYU Law Rev. Vol. 84, No. 4 p. 1396

The second way to invalidate a Glomar response is by proving that the agency acted in bad faith or concealed violations of the law.[96] This is even more difficult to prove than the official acknowledgment doctrine because the court will presume that the agency's response is legitimate if it is plausible and logical. The burden of proof for showing bad faith is on the requestor, who will always be subject to information asymmetry. Importantly, even where the agency carries out ostensibly illegal programmes, such as the NSA wiretapping without a warrant, the DC District Court found that "[e]ven if the [wiretapping programmes] were ultimately determined to be illegal, it does not follow that the NSA's decision regarding the classification of materials relating to the [wiretapping programmes] was made in order to conceal violations of law."[97] Therefore, even if an FOIA request is made to uncover violations of law and there is good evidence to suggest that the law is being violated, the Courts are still reticent to find that the classification of the documents is to conceal the law-breaking and not for other national security purposes.

C) Public Interest In Personal Privacy Exemption Cases

Even if there is a cognizable privacy interest, a Glomar response can be invalidated when there is public interest in disclosure. Although it has been held that there is balancing to be done, the identities of those investigated of charges must be protected unless "exceptional interests militate in favour of disclosure."[98] Misconduct by senior government officials such as misappropriation of government funds is a "textbook example of information the FOIA would require to be disclosed."[99]

Public Discourse Concerning NCND

In exchanges between politicians or agency spokespeople and the public, there is no general legal requirement to disclose information upon request. The Freedom of Information Act is a federal law that requires full or partial disclosure of documents controlled by the US Government when citizens submit requests pursuant to the FOIA. When an agency gives a NCND response, it is saying that it cannot release whether or not it has records. When an individual gives a verbal NCND response to a question, it is refusing to provide a response to an allegation. A search of "Neither Confirm Nor Deny" in the Washington Post, USA Today, New York Times, Los Angeles Times, and Wall Street Journal turned up very little, which suggests that politicians and spokespeople do not frequently use the language of NCND to respond to allegations.

Recently, use of the Glomar response tethered to national security has been publicised and litigated in light of two programmes.

---

[96] Wilner, 592 F.3d at 75
[97] *People for the Am. Way Found. v. NSA*, 462 F. Supp. 2d 21, 29–31 (D.D.C. 2006)
[98] *Congressional News Syndicate v United States Department of Justice* 348 F. Supp. [at 545]
[99] *Cochran v United States* 770 F.2d 949 (11th Circ 1985) [at 957]

1) The NSA Surveillance Programme:
After classified leaks by National Security Agency ('NSA') employee Edward Snowden in 2013[100] the NSA had an 888% increase in FOIA inquiries where American citizens asked whether there were records on their phone calls, phone numbers, e-mail addresses, IP addresses and if so, to access them.[101] Pamela Phillips, the chief of the NSA Freedom of Information Office said this was largest spike in FOIA requests the NSA has ever had. No significant cases have been brought forward to challenge these responses and any case would likely be unsuccessful.

2) The CIA Drone Programme:
The United States is known to have conducted drone programmes in six countries. The programmes in combat zones, Afghanistan, Iraq, and Libya, were publicly acknowledged and conducted by the Pentagon and Joint Special Operations Command. At the same time, there were programmes in Pakistan, Somalia, and Yemen that were conducted by the CIA and not publicly acknowledged for both political and strategic reasons. The official acknowledgment doctrine was successfully used to counter a Glomar response in *ACLU v CIA* concerning the CIA Glomar response to the drone programme. Because the Director of the CIA had made speeches about drones (though not about their use by the US as part of a targeted killing programme), it was highly implausible that the CIA had no documents related to drones. In the D.C. Circuit Court of Appeals Garland J held:

> "The *Glomar* doctrine is in large measure a judicial construct, an interpretation of FOIA exemptions that flows from their purpose rather than their express language. In this case, the CIA asked the courts to stretch that doctrine too far — to give their imprimatur to a fiction of deniability that no reasonable person would regard as plausible. 'There comes a point where ... Court[s] should not be ignorant as judges of what [they] know as men' and women. [*Watts v. Indiana*, 338 U.S. 49, 52, 69 S.Ct. 1347, 93 L.Ed. 1801 (1949) (opinion of Frankfurter, J.)]. We are at that point with respect to the question of whether the CIA has any documents regarding the subject of drone strikes."[102]

The D.C. Circuit Court of Appeals then remanded the case to the District Court and the ACLU narrowed the original FOIA request to just include legal analysis about authorization of the drone strikes, and information about who can be targeted and killed by the programme. The District Court then ruled that the

[100] http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data
[101] http://www.usatoday.com/story/news/nation/2013/11/17/nsa-grapples-with-988-increase-in-open-records-requests/3519889/
[102] *ACLU v CIA* 710 F.3d 422 (2013) at 431.

documents were classified and therefore the CIA was legitimate in using the Glomar response. The ACLU appealed the decision in July 2015. The outcome of the case remains pending.

Oversight and Accountability

The Federal FOIA Ombudsman is the Office of Government Information Services (OGIS). However, due to the nature of the Glomar response and the significant amount of leeway agencies are given to determine whether or not information is properly classified, the OGIS does not deal with Glomar responses. A search of the OGIS library turns up only one short page concerning the Glomar response,[103] which is merely informational and does not give any information about standards or reasons to appeal other than a brief explanation of the Official Acknowledgment doctrine. NGOs are more useful in this regard, with the ACLU undertaking significant litigation on Glomar and being the most active watchdog in civil society.[104] In addition, the Reporters Committee for Freedom of the Press gives some guidance on using "overriding public interest" to invalidate a Glomar response tied to 7(c) personal privacy but nothing else.[105]

Summary

(i) When (in relation to what subject matters) and by whom is NCND commonly deployed?

In the United States, the Freedom of Information Act (FOIA) provides citizens with a general right to request and obtain access to federal agency records. There are a variety of exceptions contained in the FOIA that allow the agency to deny the release of the records, but all statutory responses require the agency to state whether or not the records exist. The "Glomar Response" was created by common law and allows federal agencies to neither confirm nor deny the existence of the responsive records. NCND only exists in relation to FOIA, and the agency must 'tether' the NCND response to one of nine statutory FOIA exceptions. NCND responses have been accepted in relation to "unwarranted invasion of personal privacy" and "national security".

NCND responses tied to "unwarranted invasion of personal privacy" have tended to be given by Federal Bureau of Investigation in relation to the question of whether an individual has been the subject of an investigation. The subject matter of FOIA requests that have been met with NCND responses tied to "national security" have been wide-ranging, from military plans or weapons systems, foreign relations, intelligence activities, the production or location of weapons of mass destruction.

[103] https://ogis.archives.gov/the-ogis-library/glomar_s1_p389.htm.

[104] A brief summary of ACLU Glomar litigation can be found here: https://www.aclu.org/blog/what-does-soviet-submarine-have-do-us-government-secrecy

[105] http://www.rcfp.org/federal-foia-appeals-guide/exemption-7/ii-harm-disclosure/c-7c/iii-glomar-response.

(ii) What concerns have been raised over the use of NCND, if any, and by whom?

Virtually all concerns have been raised in relation to national security, and in particular the CIA's unwillingness to disclose even the most public of information, such as the very existence of a drone programme, or the existence of records relating to mass-surveillance pursuant to the Snowden leaks.

(iii) What controls or oversight, if any, is there of the use of NCND policy? Or, what controls or oversight have been recommended, and by whom?

The primary control on the use of NCND is the courts. A NCND response can be invalidated in three ways: if the agency has "officially acknowledged" the existence of the record, if it can be proven that the agency acted in bad faith or concealed violations of the law, and if disclosure is in the public interest (but this has only been successful in personal privacy cases, because an agency acting to preserve the national security is in the public interest). The Federal FOIA Ombudsman is the Office of Government Information Services (OGIS). However, due to the nature of the Glomar response and the significant amount of leeway agencies are given to determine whether or not information is properly classified, the OGIS does not deal with Glomar responses. A search of the OGIS library turns up only one short page concerning the Glomar response, which is merely informational and does not give any information about standards or reasons to appeal other than a brief explanation of the Official Acknowledgment doctrine. NGOs are more useful in this regard, with the ACLU undertaking significant litigation on Glomar and being the most active watchdog in civil society. The Reporters Committee for Freedom of the Press which gives some guidance on using "overriding public interest" to invalidate a Glomar response tied to 7(c) personal privacy but nothing else.

Australia

Public Discourse Concerning NCND

Intelligence services and operations

The Australian Intelligence Community is comprised of six intelligence agencies, including the Australian Security Intelligence Organisation (**ASIO**), the Australian Secret Intelligence Service (**ASIS**) and the Australian Signals Directorate (**ASD**).[106] Australian governments have historically operated a clear NCND policy in relation to intelligence services' operations.

The NCND policy in respect of intelligence and security matters in Parliamentary debates has been affirmed by a number of Royal Commissions. In 1977, the Royal Commission on Intelligence and Security, led by Justice Robert Hope, recommended in respect of Parliamentary responsibility:[107]

> "That the present practice, whereby the Prime Minister and the Minister administering the ASIO Act do not confirm or deny any allegations, or presumed allegations, in respect of ASIO, continue in force."

Again, in 1984, the Royal Commission on Australia's Security and Intelligence Agencies, also led by Justice Hope, recommended that the Attorney-General's practice of neither confirming nor denying any allegations or presumed allegations in Parliament should continue.[108]

In 1994, the Commission of Inquiry into the Australian Secret Intelligence Service was appointed, headed by Justice Gordon Samuels and Michael Codd. At that point, ASIO was operating under legislation,[109] but ASIS was not. The public edition of the Samuels and Codd inquiry report was released in March 1995.[110] The report recommended a legislative basis for ASIS (noting that an argument against legislation was that "it would represent a significant move away from the [NCND] policy which is essential to security").[111] It also noted that the NCND policy adopted by successive governments and accepted by successive parliaments was a significant limit on parliamentary oversight

---

106 ASIO collects intelligence within Australia, ASIS collects intelligence in foreign countries and ASD collects signals intelligence.
107 Royal Commission on Intelligence and Security, *Fourth Report*, *Volume 1* (Commonwealth Government Printer, Canberra, 1978) 259–260.
108 Royal Commission on Australia's Security and Intelligence Agencies, *Report on the Australian Security Intelligence Organisation* (Australian Government Publishing Service, Canberra, 1985) 337.
109 Australian Security Intelligence Organisation Act 1979 (Cth).
110 Commission of Inquiry into the Australian Secret Intelligence Service, *Report on the Australian Secret Intelligence Service: Public Edition* (Australian Government Publishing Service, Canberra, 1995).
111 ibid paras 2.29–2.30 and 3.28.

over ASIS, but continued to support there being governmental discretion to apply a NCND policy in parliamentary debate or elsewhere.[112]

The report then looked more closely at the NCND policy adopted for media enquiries. It said:[113]

> "The standard response to media stories has been for the Minister to state that the government neither confirms nor denies the statement being made about the Service. The practice has thus become known as 'neither confirm nor deny' (NCND). The reasoning is obvious enough: to confirm an accurate allegation would convert mere assertion into official fact, while to deny an untruthful allegation would imply confirmation of any subsequent allegation which was not denied. We examine the NCND policy more closely below. What is significant here is the uninformative and unresponsive attitude which NCND epitomises."

The issue with non-engagement with the media was that wildly inaccurate and negative information about ASIS in the media had to and could go unchallenged, which damaged morale within ASIS.[114] Further, silence in the face of repeated assertions about ASIS could be taken as confirmation.[115] Generally, the report supported a modified use of the NCND policy, stating:[116]

> "There will often be circumstances, concerning operationally sensitive information or allegations, where the appropriate response from any Government will be NCND. But if this media policy is applied in a blanket fashion, it is severely limiting for the reasons we have mentioned earlier."

The report referred to ASIO's practice of issuing selective denials when the "allegations are inflammatory and likely to cause conflict in the wider Australian community", but considered that selective denials "tend to undermine NCND in the long term" because unrebutted allegations could then be inferred to be true and allow information about ASIS operations to be gleaned by a process of elimination.[117] The report noted that a more coherent public information strategy was required, through a public information booklet and programme, based on the legislation.[118]

Both the first Hope Royal Commission and the Samuels and Codd inquiry recommended a legislative basis for ASIS. Consequently, the Intelligence Services Bill 2001 was drafted, which ultimately resulted in the Intelligence Services Act 2001 (Cth) (**ISA**).

---

[112] ibid para 3.38.
[113] ibid para 15.9.
[114] ibid paras 15.10–15.11, 15.65.
[115] ibid para 15.65.
[116] ibid para 15.66.
[117] ibid para 15.68.
[118] ibid paras 15.71–15.76.

The Bills Digest for the Intelligence Services Bill stated that the purpose of the legislation was to provide a legislative basis for the ASIS (and to a more limited extent, the Defence Signals Directorate), and to establish a joint parliamentary committee to oversee both ASIO and ASIS.[119] The Digest also set out the background leading to the proposed legislation. In relation to NCND, it observed that the Australian government's position on secrecy surrounding ASIS has relaxed over time. It quoted from the Prime Minister's Ministerial Statement of 1977, which stated:[120]

> "ASIS's capacity to serve Australia's national interest will continue to depend upon its activities being fully protected by secrecy. The Government will therefore adhere strictly to the practice of refusing to provide details of ASIS's activities nor will it be prepared to enter into any discussion on the Service."

This was compared to the following statement of the Minister for Foreign Affairs in 1995:[121]

> "[W]hile we judge that it is now an appropriate time to be more forthcoming than we have been in the past, there is still a self-evident need for certain kinds of information relating to ASIS ... to remain secret so as to protect national security, the safety of individuals, and Australia's international relations. This especially includes information that could identify ASIS officers, sources and methods; places of ASIS deployment and operation; areas and issues of intelligence interest; and the purpose or objectives of individual operations, be they past, current or projected."

This trend is also reflected in the approaches taken by the Hope Royal Commission and the later Samuels and Codd inquiry. The Bills Digest noted:

> "Ultimately, while the government has traditionally adopted a 'neither-confirm-nor-deny' approach, circumstances have ensured that at least some aspects of intelligence services' operations are questioned by the media and by parliamentarians. Obviously, the disclosure of information by former officers and journalists has prompted the most significant public debate. However, as a result of the Hope Royal Commissions, some disclosure and scrutiny has also been prompted by the ability of Parliament to review ASIS appropriations, ANAO audit reports and IGIS annual reports. There has also been an arrangement whereby ASIS

---

[119] Bills Digest No 11 2001–2002 (available at < http://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/bd/bd0102/02bd011#Passage>, accessed 7 January 2016).

[120] Malcolm Fraser, "Royal Commission on Intelligence and Security", Ministerial Statement, House of Representatives, *Debates*, 25 October 1977, 2339.

[121] Senator Gareth Evans, "Australian Secret Intelligence Service", Ministerial Statement, Senate, *Debates*, 1 June 1995, 716.

> provides briefings to the Opposition. In addition, the courts have indicated that at least some activities and decision making within the intelligence services agencies will be susceptible to judicial scrutiny (see below)."

Case authorities on secret evidence, officer immunity, extraterritorial jurisdiction and the ability to judicially review ASIS's activities were then discussed.

As per the purposes set out in the Bills Digest, the ISA set out the functions of ASIS[122] and introduced a measure of Parliamentary oversight,[123] while maintaining secrecy in relation to certain types of information.[124] The arrangement where ASIS briefs the leader of the Opposition about matters relating to it was formalised as a statutory requirement.[125] The ISA also established the Parliamentary Joint Committee on Intelligence and Security (**PJC**)[126] and set out its review functions, powers and obligations.[127] However, the PJC must not require the disclosure of "operationally sensitive information or information that would or might prejudice Australia's national security or the conduct of Australia's foreign relations".[128] While the PJC has the power to obtain information and receive evidence,[129] the responsible Minister may prevent or restrict the provision of operationally sensitive information by issuing a certificate, which cannot be questioned in any court or tribunal.[130] There are also restrictions on what can be disclosed in a report to Parliament.[131] The ISA introduces offences for unauthorised communication, recording and dealing with information (as a staff member of an agency in the Australian Intelligence Community),[132]and unauthorised disclosure or publication of information provided to the PJC or obtained as a member of the PJC.[133]

Despite the ISA, the lack of Parliamentary accountability in this area continues to be criticised by academics in the counter-terrorism context. Carne observes that Australia's human rights protections rely on the role of representative and responsible government, and states:[134]

> "Such reliance upon classic parliamentary doctrines and institutions is, in the context of national security questioning and detention powers, highly problematic. Substantial inadequacies in accountability include the often cited, bipartisan ministerial

---

122 Intelligence Services Act 2001 (Cth), Part 2.
123 ibid ss 19, 28–32 and sch 1.
124 ibid sch 1, parts 1 and 2.
125 ibid s 19.
126 ibid s 28.
127 ibid s 29–31.
128 ibid sch 1, cl 1.
129 ibid sch 1, cl 2–3 and 5.
130 ibid sch 1, cl 4.
131 ibid sch 1, cl 7.
132 ibid ss 39–41B.
133 ibid sch 1, cl 9 and 12.
134 Greg Carne, 'Gathered Intelligence or Antipodean Exceptionalism?: Securing the development of ASIO'S detention and questioning regime' (2006) 27 Adel L Rev 1, 18–19.

> response of not commenting on matters of national security (in this instance, questioning and detention warrants, providing further dimensions to the prohibitions on primary and secondary disclosure of warrant and operational information, … not commenting upon "operational matters" (as defined by the commentator, the Commonwealth Attorney-General) and the use of the Glomar response "to neither confirm nor deny" matters relating to national security. The Attorney-General is then able to become the sole source of authorised public disclosures of information on the operation of the warrants, thereby able to control debate and accountability through selective release of information and invoke "operational matters" as a rationalisation for declining further disclosure."

Recent examples of the NCND policy in respect of intelligence or security operations can be found in Parliamentary debates, although it is usually used in a "no comment" sense. Two recent examples are transcribed below:

"Senate Estimates of the Foreign Affairs, Defence and Trade Legislation Committee on 22 October 2014:[135]

> **Lt Gen. Morrison**: With respect, I will not be making any comment about that.
>
> **Senator LUDLAM**: So that is a 'neither confirm nor deny' sort of—
>
> **Air Chief Marshal Binskin**: We will not talk about special forces and their capabilities, for obvious reasons.
>
> **Senator LUDLAM**: I have not even started on capabilities and I do not want to trespass into operational stuff, but it does not seem unreasonable to be able to ask whether such a squadron even exists or not. Is that not something that the parliament would have a right to know?
>
> **Air Chief Marshal Binskin**: We will not talk about special forces capabilities in an open forum.

Senate Estimates of the Legal and Constitutional Affairs Legislation Committee on 24 February 2014:[136]

> **Senator LUDLAM**: If I did bring you something that was pure fabrication you would have no difficulty in shutting it down. I am bringing to you an instance different from the one where we

[135] Hansard *Senate Foreign Affairs, Defence and Trade Legislation Committee Estimates* (22 October 2014) 134.
[136] Hansard *Senate Legal and Constitutional Affairs Legislation Committee Estimates* (24 February 2014) 75.

> allegedly spied on the Timorese cabinet. Could you confirm or deny whether we had lawyers from the United States who were engaged by the government of Indonesia in trade negotiations relating to prawn and clove cigarette exports?
>
> **Senator Brandis**: I cannot do any better than repeat my earlier answer.
>
> **Senator LUDLAM**: But there was not an answer to repeat.
>
> **Senator Brandis**: Without conceding the premise of your question, my answer was that the government neither confirms, denies nor comments on intelligence matters."

In terms of media policy, there appears to have been a move away from the language of NCND to a "does not comment" position. For example, in ASIO's reports to Parliament, from approximately 1997 to 2001, it included the following statement (or similar) about its media policy:[137]

> "In response to media allegations and questions, ASIO has a general policy of 'neither confirm nor deny'. In some circumstances, however, the Attorney-General (or the Director-General with the Minister's agreement) may decide to issue a statement of denial or clarification to the media, where it is in the interests of promoting public confidence in the legality, propriety and effectiveness of ASIO's conduct and management."

From 2002 onward, ASIO changed the wording such that its media policy was that it "does not normally comment on matters of national security".[138] In its most recent report, ASIO stated that it "routinely responds to media enquiries but does not comment on operations, investigations or individuals, nor does it comment on operational capabilities".[139]

Recent examples in the media of the NCND response for intelligence matters include allegations in 2013 that Australia had spied on East Timor and Indonesia. In a statement responding to spying on East Timor, the Foreign Affairs Minister and the Attorney-General said that "it had been the position of successive Australian governments to neither confirm nor deny [the allegations]".[140] In relation to claims of spying on Indonesia after the Edward Snowden disclosures, Prime Minister Tony Abbott also maintained a NCND approach. The article states:[141]

---

[137] Australian Security Intelligence Organisation, *ASIO Report to Parliament 1997–1998* (1998) 27; Australian Security Intelligence Organisation, *ASIO Report to Parliament 2000–2001* (2001) 51.
[138] Australian Security Intelligence Organisation, *ASIO Report to Parliament 2002–2003* (2003) 52.
[139] Australian Security Intelligence Organisation, *ASIO Report to Parliament 2014–2015* (2015) 61.
[140] Dan Harrison, 'East Timor seeks to sink sea treaty over spy claims' (*Sydney Morning Herald*, 4 May 2013) <http://www.smh.com.au/national/east-timor-seeks-to-sink-sea-treaty-over-spy-claims-20130503-2iyrt.html> accessed 17 December 2015.
[141] Tom Allard and Michael Bachelard, 'Neighbourhood watch: how Indonesia and Australia faced off over spying claims' (*Sydney Morning Herald*, 23 November 2013)

> "His approach to neither confirm nor deny the surveillance has been the bipartisan orthodoxy and no doubt reflected the advice of his foreign affairs and intelligence chiefs. It is a long-standing convention and Michael Wesley, a professor at the ANU College of National Security, says it has served Australia well.
>
> "It's a slippery slope," he says. "Once you make an admission, you open yourself up to having to do it again and again in the future."'

The Australian government has also taken a NCND stance in the media in relation to other politically contentious issues involving foreign affairs, such as whether Australia had paid people smugglers to return to Indonesia.[142]

Investigations by financial regulator

The Australian Securities & Investments Commission (**ASIC**) also has a form of NCND policy for its ongoing investigations. On its website, in its information sheet 152 titled 'Public comment on ASIC's regulatory activities',[143] it states that it will make a statement about an investigation when it is in the public interest to do so, but that:

> "Where the risk of damage to an individual from the publicising of an investigation is high, that will often result in a decision not to confirm or deny that we are investigating a matter until further facts about the alleged misconduct can be gathered, analysed and tested."

The Governance Institute of Australia referred to this policy as precluding public understanding in its submission to the Senate Economics References Committee in 2013. It stated: [144]

> "Governance Institute of Australia notes that ASIC is often viewed as acting tentatively in investigating and enforcing matters, yet under its legislative framework, ASIC will neither confirm nor deny that an investigation is underway unless it is in the public

---

<http://www.smh.com.au/national/neighbourhood-watch-how-indonesia-and-australia-faced-off-over-spying-claims-20131122-2y1f8.html> accessed 17 December 2015.

[142] See Shalailah Medhora, 'Tony Abbott sticks to 'stop the boats' in face of claims people smugglers paid' (*The Guardian*, 14 June 2015) <http://www.theguardian.com/australia-news/2015/jun/14/tony-abbott-sticks-to-stop-the-boats-in-face-of-claims-people-smugglers-paid> accessed 17 December 2015; Marie McInerney, 'Migrant boat allegations cast cloud over Australia' (*BBC News*, 15 June 2015) <http://www.bbc.co.uk/news/world-australia-33130707> accessed 17 December 2015.

[143] Australian Securities & Investments Commission, 'Public comment on ASIC's regulatory activities' (June 2015) <http://asic.gov.au/about-asic/asic-investigations-and-enforcement/public-comment-on-asics-regulatory-activities/> accessed 17 December 2015.

[144] Governance Institute of Australia, 'Inquiry into the Performance of the Australian Securities and Investments Commission' (Letter to the Senate Economics References Committee, 21 October 2013) 4.

> interest to do so. Confidentiality of surveillance and investigation is central to preserving the integrity of the market, but it results in external public parties being unable to objectively evaluate ASIC's actions."

Examples of where ASIC has utilised a NCND response in the media include responding to whether there was an investigation into a breach of employee share sales rules by Foster's Group,[145] and commenting on the execution of a ASIC search warrant (noting that it was "[ASIC's] policy to neither confirm nor deny the execution of search warrants").[146]

Statutory framework for information requests (Commonwealth)

For the Australian government and federal Australian agencies, the Freedom of Information Act 1982 (Cth) (**FOIA**) applies to requests for information. The FOIA contains a statutory provision permitting an agency neither to confirm nor deny the existence of a document in certain cases. Section 25 states:

> **25 Information as to existence of certain documents**
>
> (1) Nothing in this Act shall be taken to require an agency or Minister to give information as to the existence or non-existence of a document where information as to the existence or non-existence of that document, if included in a document of an agency, would cause the last-mentioned document to be:
>
> (a) an exempt document by virtue of section 33 or subsection 37(1) or 45A(1); or
>
> (b) an exempt document to the extent referred to in subsection 45A(2) or (3).
>
> (2) If a request relates to a document that is, or if it existed would be, of a kind referred to in subsection (1), the agency or Minister dealing with the request may give notice in writing to the applicant that the agency or the Minister (as the case may be) neither confirms nor denies the existence, as a document of the agency or an official document of the Minister, of such a document but that, assuming the existence of such a document, it would be:

[145] James Chessell and Lisa Murray, 'Foster's exec out for selling shares' (*Sydney Morning Herald*, 28 January 2005) <http://www.smh.com.au/news/Business/Fosters-exec-out-for-selling-shares/2005/01/27/1106415733046.html> accessed 17 December 2015.

[146] Rebecca Urban, 'Police seize executives' computers in raid on Genetic Technologies' (*The Age*, 8 March 2007) <http://www.theage.com.au/news/business/police-seize-executives-computers-in-raid-on-genetic-technologies/2007/03/07/1173166799276.html> accessed 17 December 2015.

(a) an exempt document by virtue of section 33 or subsection 37(1) or 45A(1); or

(b) an exempt document to the extent referred to in subsection 45A(2) or (3).

(3) If a notice is given under subsection (2) of this section:

(a) section 26 applies as if the decision to give the notice were a decision referred to in that section; and

(b) the decision is taken, for the purposes of Part VI, to be a decision refusing to grant access to the document in accordance with the request referred to in subsection (2) of this section, for the reason that the document would, if it existed, be:

(i) an exempt document by virtue of section 33 or subsection 37(1) or 45A(1); or

(ii) an exempt document to the extent referred to in subsection 45A(2) or (3).

Sections 33, 37 and 45A come under the heading "Exemptions". They provide for what are called "exempt documents". Section 33 states that a document is exempt if its disclosure "would, or could reasonably be expected to, cause damage to" the security, defence or international relations of the Commonwealth of Australia, or would divulge information communicated in confidence by or behalf of a foreign government or international organisation. Section 37 provides that documents affecting the enforcement of law and protection of public safety are exempt documents, and s 45A provides that Parliamentary Budget Office documents are exempt.

Section 26(1) requires the agency to give notice in writing of the decision, including findings on any material questions of fact and the reasons for the decision. A statement of reasons should not include any information that, if it were in a document, would cause that document to be exempt (s 26(2)).

It is noted that the above FOIA regime does not apply to Australian intelligence agencies. Section 7 of the FOIA exempts certain persons and bodies from the operation of the Act, which include the six Australian Intelligence Community agencies (including ASIS, ASIO and ASD).[147] The Parliamentary Budget Office is also exempted. There is thus no procedure allowing individual information requests from these agencies.

[147] See Freedom of Information Act 1982, s 7 and Schedule 2.

Commentary, reports and guidance on statutory framework for information requests (Commonwealth)

Coppel explains that the FOIA uses the idea of a notional document containing information as to the existence of documents answering the terms of the request.[148] If that notional document would itself be an exempt document under ss 33, 37 or 45A, then the agency is not required to confirm or deny the existence of the actual documents.

The Australian Information Commissioner can issue guidelines about the operation FOIA under s 93A. These were published in December 2010 and revised in October 2014.[149] The guidelines note that the act of confirming or denying the existence of a document can sometimes cause damage similar to disclosing the document itself. It gives examples of an investigation being thwarted by a suspect knowing about the existence of a current telecommunications interception warrant,[150] or disclosure of a confidential source resulting from knowing that an agency possesses a document.[151] The guidelines also state that "agencies and ministers should use s 25 only in exceptional circumstances",[152] and "resort to s 25 should be reserved strictly for cases where the circumstances of the request require it".[153]

Section 25 had been considered by the Australian Law Reform Commission in its 1995 review of the FOIA.[154] It stated:[155]

> "The provision is designed to allow agencies to withhold information about the existence (or non-existence) of a document where that information is itself exempt. For example, the fact that there is no document about Australia's nuclear weapons capabilities may be considered worth protecting under s 25 if knowledge of that fact would enable an applicant to undermine national security. … Section 25 is especially problematic for applicants because it appears to perpetuate the kind of secretive, conspiratorial agency culture that the FOI Act is intended to break down. DP 59 asked whether there is a problem with the 'neither confirm nor deny' response provided for by s 25. A number of submissions consider that s 25 is contrary to the spirit of the Act and should be repealed. Others consider it a necessary provision."

---

148 Phillip Coppel, *Information Rights: Law and Practice* (4th edn, Hart Publishing, 2014) para 2-013.
149 Office of the Australian Information Commissioner, *Guidelines issued by the Australian Information Commissioner under s 93A of the Freedom of Information Act 1982* (December 2010, revised October 2014).
150 ibid para 3.93.
151 ibid para 5.42.
152 ibid para 3.95.
153 ibid para 5.44.
154 Law Commission, *Open Government - A Review of the Federal Freedom of Information Act 1982* (ALRC Report 77, 1996).
155 ibid para 8.21.

The Commission expressed concern that "s 25 can be used to 'bamboozle' applicants with legalistic jargon", but nevertheless concluded that:[156]

> "unfortunately, the provision is necessary where information about the existence (or non-existence) of a document needs to be withheld. However, reliance on s 25 will only be justified in rare situations."

It continued, stating:[157]

> "… the FOI Commissioner should educate agencies about the correct use of s 25 and monitor their practices to ensure that agencies do not exploit it or claim it when it is the contents of a document, rather than its existence that warrants protection. Agencies may choose to seek the advice of the FOI Commissioner as to whether it would be proper to use s 25 in a particular instance."

The FOIA had previously contained a s 33A, which provided that documents that would or could cause damage to relations between the Commonwealth and a State or would divulge information communicated in confidence between them were exempt documents. There was the power to neither confirm nor deny the existence of such documents as s 33A was included in s 25.[158]

The Commission did not consider a s 25 response justified in relation to Commonwealth/State relations, noting that it could not envisage any situation in which releasing information about the existence or non-existence of a document would cause damage to domestic inter-government relations. In relation to s 25, the Commission recommended that:

- The s 25 response not be available in respect of such documents about Commonwealth/State relations; and
- The FOI Commissioner should educate agencies about the correct use of s 25.

As a result of those recommendations, and following a number of other reviews of the FOIA,[159] the reference to s 33A in s 25 was removed by the Freedom of Information

---

156 ibid para 8.22.

157 ibid.

158 At the time of the Law Commission's review in 1995, s 25(1) of the FOIA stated: "… would cause the last-mentioned document to be an exempt document by virtue of section 33 or 33A or subsection 37(1)", and s 25(2) of the FOIA stated: "… it would be an exempt document under section 33 or 33A or subsection 37(1) …".

159 These include reviews by the Commonwealth Ombudsman in 1999 and 2006, and by the Australian National Audit Office in 2004, which did not discuss the operation of s 25 of the FOIA.

Amendment (Reform) Act 2010 (Cth), thereby removing the availability of the NCND response in relation to documents relating to Commonwealth/State relations.[160]

Judicial discussion around the use of s 25 will be considered in the third section below.

Statutory framework for information requests (States and Territories)

Other Australian States and Territories have equivalent legislation for state governments and agencies with corresponding NCND provisions. Some of these are worded very similarly to s 25 of the FOIA, while others are less detailed. These are:

- *Australian Capital Territory*: Freedom of Information Act 1989 (ACT), s 24.
- *New South Wales*: Government Information (Public Access) Act 2009 (NSW), s 58(1)(f).
- *Northern Territory*: Information Act 2002 (NT), ss 21(4) and 24(3).
- *Queensland*: Right to Information Act 2009 (Qld), s 55 (previously Freedom of Information Act 1992 (Qld), s 35).
- *South Australia*: Freedom of Information Act 1991 (SA), s 23(3).
- *Tasmania*: Right to Information Act 2009 (Tas), s 22(4).
- *Victoria*: Freedom of Information Act 1982 (Vic), ss 27(2)(b) and 33(6).
- *Western Australia*: Freedom of Information Act 1992 (WA), s 31.

These provisions all permit agencies to use a NCND response generally for reasons of security, law enforcement or when it is in the public interest. An unusual exception is s 33(6) of the Victoria legislation, which allows an agency to provide a NCND response where disclosure would "involve the unreasonable disclosure of information relating to the personal affairs of any person (including a deceased person)".[161]

What accountability bodies outside of the courts have discussed NCND?

I have not been able to locate any discussion of NCND by accountability bodies aside from those mentioned in the sections above.

---

[160] Freedom of Information Amendment (Reform) Act 2010 (Cth), s 18. Section 33A was also repealed and substituted by a new s 47B, which designated Commonwealth/State relations documents as conditionally exempt (requiring a public interest test to be met) instead.

[161] Freedom of Information Act 1982 (Vic), s 33(1). See Mick Batskos, 'Balancing the Treatment of 'Personal Information' under FOI and Privacy Laws: a Comparative Australian Analysis: Part 2' (paper presented at the AIAL 2014 National Administrative Law Conference, Perth, 25 July 2014) 79.

Is there any judicial treatment or discussion of NCND?

Cases under s 25 of the FOIA (Commonwealth)

Cases involving s 25 of the FOIA indicate that tribunals and courts do not always readily accept that a NCND response is necessary. In *Department of Community Services v Jephcott*,[162] the Federal Court of Australia upheld a decision of the Administrative Appeals Tribunal directing that the Department of Health inform the requester, Mrs Jephcott, as to the existence or non-existence of the documents the subject of her request.

In that case, Mrs Jephcott, who received a domiciliary nursing care benefit for her mother, requested records held by the Department of Health on her given by her sister. She suspected that her sister had given disparaging information about the level of care she had provided to the Department. The Department refused to confirm or deny the existence of such documents under the exemption on disclosing the identity or existence of a confidential source (s 37(1)(b)). The Tribunal held that for s 25 to be employed, there needed to be some evidence that in the event of a confirmation or denial, the requester would then use a technique to deduce the identity or existence of a confidential source of information. There was no evidence that Mrs Jephcott was doing so as she already suspected that her sister had provided information to the Department. The Federal Court upheld the Tribunal's reasoning.

In *Secretary, Department of Health and Aging v iNova Pharmaceuticals (Australia) Pty Ltd*,[163] the Federal Court discussed the relationship between ss 25 and 26. It held that, notwithstanding s 25, in a notice issued under s 26(1), the agency can deny the existence of any document exempted by the Act. It would be anomalous if the agency were required to disclose whether a document existed or not in its s 26 notice to the requester, having invoked s 25.[164] Disclosure of the non-existence of the documents could lead to discovery of the existence of documents if periodic requests were made over time and the form of the response changed.[165]

Cases from the Queensland Information Commissioner

A case in which there was significant discussion of NCND under the statutory framework on freedom of information is *Est v Department of Family Services & Aboriginal & Islander Affairs*.[166] The Queensland Information Commissioner held that the NCND response should be reserved for use "only where special circumstances make its use necessary and appropriate".

The applicant there had requested from the Department of Family Services and Aboriginal and Islander Affairs copies of complaints made against him by two

---

[162] (1987) 15 FCR 122 (FCA).
[163] (2010) 191 FCR 573 (FCA).
[164] ibid para [58]–[65].
[165] ibid para [62].
[166] [1995] QICmr 20.

individuals, which he believed were libellous. The relevant provision in force then was s 35 of the Freedom of Information Act 1992 (Qld). Instead of the idea of whether the notional document (if existing) is exempt, as per s 25, s 35 of the Queensland Act refers to whether there is or would be exempt matter in a requested document if it exists.

The Commissioner then referred to the 1979 report by the Senate Committee on Constitutional and Legal Affairs on the draft Commonwealth Freedom of Information Bill and the Queensland Electoral and Administrative Review Commission,[167] both of which highlighted the power to use a NCND response is open to potential misuse and ought to be confined to "a very narrow set of exemptions", namely the classes of documents whose character is recognised as being especially sensitive or requiring particular secrecy.

Examples were given of when a s 35 response was appropriate: where a person is trying to ascertain whether someone had informed on them (such as by using a 'shopping list' approach in making similarly framed requests in respect of a number of suspected informers), and in areas of government administration, where a group of persons making a series of access applications at regular intervals can ascertain the information held by an agency through changes in the responses given.[168]

The Commissioner went on to state:[169]

> "As the legislative history indicates, resort to s.35 was intended to be the exception rather than the rule. The normal response should be to acknowledge the existence of requested documents which contain matter claimed to be exempt under s.36, s.37 or s.42, and justify the claims for exemption (or acknowledge that requested documents do not exist). The s.35 "neither confirm nor deny" response should be reserved for use only where special circumstances make its use necessary or appropriate."

More recent examples of the Queensland Information Commissioner affirming the use of the NCND response under s 55 of the Right to Information Act 2009 (Qld) include *Phyland and Department of Police*,[170] in relation to access for documents showing the criminal record of a named individual, and *3FG6LI and Queensland Police Service*.[171]

Access to Australian Archives

There has also been some judicial comment on the NCND response in the context of a case involving records exempt from public access as part of the National Archives. In *Re*

[167] ibid paras 11–12.
[168] ibid paras 13–14.
[169] ibid para 15.
[170] [2011] QICmr 35.
[171] [2014] QICmr 32.

Slater and Director-General, Australian Archives,[172] some of the contested applications for access related to certain ASIS records about Cambodia, Indonesia, West New Guinea, Malaya and Singapore, in which the Department of Foreign Affairs (on behalf of ASIS) advised that the existence of relevant records was neither confirmed nor denied in accordance with s 39 of the Archives Act 1983.[173] This was on the basis that disclosure of the information could reasonably be expected to cause damage to the security, defence and international relations of the Commonwealth,[174] and is information communicated in confidence by or on behalf of a foreign government.[175]

In discussing security under s 33(1)(a) of the Archives Act, one of the factors the Tribunal referred to is the significance of official acknowledgement, stating that "[e]ven if a fact is the subject of widespread media and public speculation, its official acknowledgement could cause damage to security".[176] In support of this the Tribunal referred to and quoted from the *Glomar* line of cases.[177]

The Tribunal also discussed many other factors in support of the records being exempt. It concluded that reasonable grounds exist for the claims made to neither confirm nor deny the existence of the documents, or to refuse access.

Summary

(i) When (in relation to what subject matters) and by whom is NCND commonly deployed?

In Australia, the language of NCND is most commonly employed in relation to intelligence services and operations, by the Australian government and intelligence services such as the Australian Secret Intelligence Service (**ASIS**) in Parliament and in the media. It is also used to a lesser extent by the financial regulator, the Australian Securities & Investments Commission (**ASIC**) in relation to investigations into potential misconduct in the financial markets. The Freedom of Information framework provides for a NCND response to information requests, which has been used by a variety of government agencies (such as the Department of Health, the Police). The information request regime does not apply to intelligence services.

[172] [1988] AATA 110, (1988) 8 AAR 403.
[173] Section 39(1) of the Archives Act 1983 is worded very similarly to s 25 of the Freedom of Information Act 1982 (Cth), stating: "Nothing in this Act shall be taken to require the Archives to give information as to the existence or non-existence of a record where information as to the existence or non-existence of that record, if included in a Commonwealth record, would cause that last-mentioned record to be an exempt record by virtue of paragraph 33(1)(a), (b) or (e)." Paragraph 33(1)(a), (b) and (e) relate to security, defence or international relations, information communicated in confidence by a foreign government or international organisation, and the maintenance of the law.
[174] Archives Act 1983, s 33(1)(a).
[175] Archives Act 1983, s 33(1)(b).
[176] *Re Slater* (n 172), para 47.
[177] *Phillippi v CIA* 655 F 2d 1325 (1981) 1332–1333; *Military Audit Project v Casey* 656 F 2d 724 (1981) 744–745 *Afshar v Department of State* 702 F 2d 1125 (1983) 1130–1131.

(ii) What concerns have been raised over the use of NCND, if any, and by whom?

In relation to intelligence services and operations, concerns were raised in more recent Royal Commission inquiries that the use of the NCND response led to inaccurate information and speculation in the media about ASIS. It was also recognised that the NCND response hindered Parliamentary accountability, although by and large the existence of some form of NCND response is considered necessary. Academic commentators are more critical of the use of NCND, noting that it contributes to the lack of accountability. Similar concerns have been raised by the Governance Institute of Australia in relation to the use of NCND by ASIC. In the Freedom of Information context, in the leading authority of *Est*, the Queensland Information Commissioner has observed that the NCND response is open to potential misuse and should only be employed in exceptional circumstances.

(iii) What controls or oversight, if any, is there of the use of NCND policy? Or, what controls or oversight have been recommended, and by whom?

Government agencies such as ASIO and ASIC have broad media policies explaining when the NCND response will be used, although there does not appear to be any independent oversight of this. In the Freedom of Information context, where NCND is officially given as a response to an information request, the response can be reviewed by the Australian or relevant State Information Commissioner.

New Zealand

Background

Before exploring public discourse concerning NCND in New Zealand, it may be useful to outline some background relevant to NCND in New Zealand's history – namely, its use by the US in relation to nuclear-armed and nuclear-powered ships. This background may inform the public perception of the use of NCND in New Zealand.

Broadly, New Zealand had adopted a nuclear-free policy, and in 1985 banned a visit by the USS *Buchanan* because the US had a NCND policy on whether their warships had nuclear capabilities.[178] This resulted in New Zealand leaving the three-way ANZUS Treaty between Australia, New Zealand and the US. The New Zealand Nuclear Free Zone, Disarmament, and Arms Control Act 1987 was then passed, banning visits by nuclear-armed and nuclear-powered ships, and requiring the Prime Minister to be satisfied that foreign warships are not carrying nuclear explosives before granting approval for their entry.[179] The US's NCND policy has always been inconsistent with the requirement that New Zealand's Prime Minister declare a warship nuclear-free before allowing it in New Zealand waters.[180]

Public Discourse Concerning NCND

There does not appear to be any area in which the New Zealand government adopts a consistent and explicit NCND policy. The phrase is most often used in the media in the surveillance context, in relation to informants or intelligence capabilities. A number of examples are set out below:

- In 2008, an article was published about police using paid informers to spy on activist groups, such as Greenpeace, animal rights and climate change campaigners.[181] The Police position was to "neither confirm nor deny the identity or existence of any informant within any group".

---

178 See generally Ministry for Culture and Heritage, 'USS Buchanan refused entry to NZ, 4 February 1985' (*New Zealand History*, 30 October 2014) <http://www.nzhistory.net.nz/page/uss-%26lt%3Bem%26gt%3Bbuchanan%26lt%3B/em%26gt%3B-refused-entry-nz> accessed 14 December 2015.

179 New Zealand Nuclear Free Zone, Disarmament, and Arms Control Act 1987, ss 9–11.

180 There are a series of working papers published by the Centre for Peace Studies analyzing the US NCND policy in relation to nuclear weapons, advocating its elimination. See, for example, Robert E White, 'The Neither Confirm Nor Deny Policy: Oppressive, Obstructive, And Obsolete' (Working Paper No. 1, Centre for Peace Studies, May 1990), available at <http://www.disarmsecure.org/The%20Neither%20Confirm%20Nor%20Deny%20Policy%20Oppressive,%20Obstructive,%20and%20Obsolete.pdf> accessed 14 December 2015.

181 Sunday Star Times, 'Anti-terror squad spies on protest groups' (*Stuff*, 13 December 2008) <http://www.stuff.co.nz/national/760969/Anti-terror-squad-spies-on-protest-groups> accessed 14 December 2015.

- In 2014, following the global surveillance disclosures by Edward Snowden relating to the Five Eyes network under the UKUSA Agreement, a NCND response was given to particular aspects of the workings of the Government Communications Security Bureau (**GCSB**). When asked about US spy facilities and intelligence programmes in New Zealand, Prime Minister John Key denied there were NSA facilities in New Zealand, and declassified top secret documents to show that a mass surveillance programme called Speargun was not being used (contrary to claims made by Glenn Greenwald), and a programme called Cortex was used instead. However, he refused to confirm whether the GCSB had access to the programme XKeyscore. The GCSB director from 2006 to 2011, Sir Bruce Ferguson, also would not confirm or deny whether the XKeyscore programme was used by the GCSB.[182]

- In 2015, further information from Edward Snowden obtained by journalist Nicky Hager indicated that the GCSB were spying on New Zealand's Pacific neighbours. Prime Minister John Key also would not confirm or deny to the media if New Zealand's spy agencies were spying in the Pacific.[183]

Nonetheless, there seems to be a recognition that openness is necessary in the surveillance field for public trust, with Howard Broad, former Police commissioner, noting that the traditional "neither confirm or deny" response "hasn't helped". He explained however that there were risks that greater unthinking disclosure could have an impact on security.[184]

Other examples of contexts in which governmental agencies have used an NCND response (or have been perceived to do so) are in relation to politically contentious investments, or investigations by financial regulators. The NZ Super Fund relied on NCND in response to an Official Information Act request,[185] and there has been a

---

[182] Tova O'Brien, 'John Key quiet on XKeyscore' (*3 News*, 16 September 2014) <http://www.3news.co.nz/politics/john-key-quiet-on-xkeyscore-2014091618#axzz3uJpgptIp> accessed 14 December 2015; 'Key silent on spy programme' (*Radio New Zealand*, 16 September 2014) <http://www.radionz.co.nz/news/political/254691/key-silent-on-spy-programme> accessed 14 December 2015.

[183] Aimee Gulliver and Michael Field, 'GCSB committing crimes against whole countries – Greens' (*Stuff*, 5 March 2015) <http://www.stuff.co.nz/national/66972448/snowden-leak-spying-claims-spark-diplomatic-fallout> accessed 14 December 2015.

[184] David Fisher, 'Why NZ spy chiefs can no longer get away with saying 'we can neither confirm or deny", (*NZ Herald*, 9 December 2014) <http://www.nzherald.co.nz/nz/news/article.cfm?c_id=1&objectid=11371394> accessed 14 December 2015.

[185] Ron Mark, 'Superfund "Neither Confirm Or Deny" Over Silver Fern Farms' (*Scoop*, 11 September 2015) <http://www.scoop.co.nz/stories/PA1509/S00212/superfund-neither-confirm-or-deny-over-silver-fern-farms.htm> accessed 14 December 2015.

perception that the previous financial regulator, the Securities Commission, operates on an NCND basis in relation to investigations into the financial markets.[186]

Statutory framework for information requests

For individual requests for information, New Zealand has a statutory basis for the refusal to confirm or deny the existence of information. These are under the Privacy Act 1993 (for personal information relating to the natural person requesting the information) and the Official Information Act 1982 (**OIA**) (for all other official information requested from government departments and organisations).[187]

Section 32 of the Privacy Act 1993 states:

> **32 Information concerning existence of certain information**
>
> Where a request made pursuant to principle 6 relates to information to which section 27 or section 28 applies, or would, if it existed, apply, the agency dealing with the request may, if it is satisfied that the interest protected by section 27 or section 28 would be likely to be prejudiced by the disclosure of the existence or non-existence of such information, give notice in writing to the applicant that it neither confirms nor denies the existence or non-existence of that information.

Principle 6 provides that if an agency holds personal information about an individual, that individual is entitled to obtain confirmation about whether personal information is held, and to access that information, subject to the application of Parts 4 and 5. Part 4 (ss 27 to 32) is headed "Good reasons for refusing access to personal information". Section 27 allows agencies to refuse to disclose information if it would prejudice the security, defence or international relations of New Zealand, the maintenance of the law or would endanger the safety of any individual, and s 28 relates to non-disclosure of trade secrets or for other commercial reasons.

Section 10 of the OIA states:

> **10 Information concerning existence of certain information**
>
> Where a request under this Act relates to information to which section 6 or section 7 or section 9(2)(b) applies, or would, if it existed, apply, the department or Minister of the Crown or organisation dealing with the request may, if it or he is satisfied

---

[186] Fiona Rotherham, 'Neither confirm, nor deny' (*Stuff*, 6 December 2010) <http://www.stuff.co.nz/business/opinion-analysis/4428436/Neither-confirm-nor-deny> accessed 14 December 2015.

[187] An equivalently worded provision also exists in s 8 of the Local Government Official Information and Meetings Act 1987 for official information held by local authorities.

that the interest protected by section 6 or section 7 or section 9(2)(b) would be likely to be prejudiced by the disclosure of the existence or non-existence of such information, give notice in writing to the applicant that it or he neither confirms nor denies the existence or non-existence of that information.

Section 6 is as follows:

6 Conclusive reasons for withholding official information

Good reason for withholding official information exists, for the purpose of section 5 of this Act, if the making available of that information would be likely—

(a) To prejudice the security or defence of New Zealand or the international relations of the Government of New Zealand; or

(b) To prejudice the entrusting of information to the Government of New Zealand on a basis of confidence by

(i) The government of any other country or any agency of such a government; or

(ii) Any international organisation; or

(c) To prejudice the maintenance of the law, including the prevention, investigation, and detection of offences, and the right to a fair trial; or

(d) To endanger the safety of any person; or

(e) To damage seriously the economy of New Zealand by disclosing prematurely decisions to change or continue Government economic or financial policies relating to

(i) Exchange rates or the control of overseas exchange transactions:

(ii) The regulation of banking or credit:

(iii) Taxation:

(iv) The stability, control, and adjustment of prices of goods and services, rents, and other costs, and rates of wages, salaries, and other incomes:

(v) The borrowing of money by the Government of New Zealand:

(vi) The entering into of overseas trade agreements.

Sections 7 and 9(2)(b) relate to special and other reasons for withholding official information. Section 7 relates to official information about the Cook Islands, Tokelau, Niue, or the Ross Dependency, and s 9(2)(b) relates to non-disclosure of trade secrets or for other commercial reasons.

In the public interest immunity context, s 27(3) of the Crown Proceedings Act 1950 states:

> **27 Discovery**
>
> …
>
> (3) Without prejudice to the proviso to subsection (1), any rules made for the purposes of this section shall be such as to secure that the existence of a document will not be disclosed if—
>
> (a) the Prime Minister certifies that the disclosure of the existence of that document would be likely to prejudice—
>
> (i) the security or defence of New Zealand or the international relations of the Government of New Zealand; or
>
> (ii) any interest protected by section 7 of the Official Information Act 1982; or
>
> (b) the Attorney-General certifies that the disclosure of the existence of that document would be likely to prejudice the prevention, investigation, or detection of offences.

Discussion of and application of the statutory framework for information requests

Privacy Commissioner and Ombudsmen

The New Zealand Privacy Commissioner website states that s 32 of the Privacy Act overrides the fundamental right of individuals to know whether or not an agency holds information about them.[188] However, it states that s 32 only applies in "very limited circumstances" and that to date it has only been raised in relation to information held by the New Zealand Security Intelligence Service (**NZSIS**) and very occasionally, the Police. It then notes that there is a two-step test before the NCND response can be used:

> (i) the release of information would be likely to prejudice the interests protected by a withholding provision; and

[188] Privacy Commissioner, 'Neither confirm nor deny' <https://privacy.org.nz/the-privacy-act-and-codes/privacy-principles/access/neither-confirm-nor-deny/> accessed 14 December 2015.

(ii) the knowledge of whether or not the agency even holds such information would have the same effect as the knowledge of the content of that information.

This two-step approach was also referred to in an Ombudsman editorial in relation to the OIA,[189] which stated:

> "There are two conditions that must be met before section 10 can apply to a request:
>
> (1) The information requested is of a kind to which any of the conclusive withholding grounds specified in sections 6 or 7 of the Act could apply, or to which those grounds of commercial prejudice specified in section 9(2)(b) of the Act could be applicable; and
>
> (2) The decision maker must be satisfied that the particular protected interest "would be likely to be prejudiced" by simple disclosure of the existence or non-existence of the requested information."

Intelligence services policies

The main organisations forming part of the New Zealand Intelligence Community are the GCSB, the NZSIS and the National Assessments Bureau within the Department of the Prime Minister and Cabinet.

The GCSB has set out its policy on responding to information requests in Policy Procedure 1007.[190] It notes that it can neither confirm nor deny the existence or non-existence of information when declaring the GCSB holding the information can prejudice the interests protected by sections 6, 7 or 9 of the OIA or sections 27 or 28 of the Privacy Act.[191] In the case of certain individuals with "identified unusual perceptions", the GCSB may choose to confirm that no information is held instead of using the NCND response under s 10 of the OIA or s 32 of the Privacy Act.[192] There is a high threshold for identifying someone as having "unusual perceptions", which is a decision made case-by-case approved by the Chief of Staff, and involves "repeated requests for information with potentially abusive/nonsensical language or requests".[193]

---

189 Office of the Ombudsman, 'To Confirm or Deny, That is the Question...' (Ombudsman Editorial Vol 2, Issue 3, 1996), available at <http://www.ombudsman.parliament.nz/ckeditor_assets/attachments/29/2-3.pdf> accessed 14 December 2015.

190 Government Communications Security Bureau, *Responding to Information Requests* (Policy Procedure 1007), available at <http://www.gcsb.govt.nz/assets/GCSB-Documents/Policy-1007-Responding-to-Information-Requests.pdf> accessed 14 December 2015.

191 ibid para 44.

192 ibid para 49.

193 ibid para 50.

The NZSIS explains why it frequently uses the NCND response. On its website,[194] it notes that:

> "The general principle of neither confirming nor denying the existence or non-existence of information, particularly in relation to investigations, allows our work to continue. The success of the investigatory work of the NZSIS relies on discretion and confidentiality.
>
> If an individual receives a "neither confirm nor deny" response, this does not necessarily mean they are of security interest. Usually, they will be of no concern to the NZSIS at all. But the unique nature of our work means we must neither confirm nor deny the existence of information broadly, in order to preserve our investigatory work."

In an attached document,[195] the NZSIS further explains that because security investigations are long-term and prospective in nature, and often covertly, disclosure of the existence of information can prejudice security.[196] It states:

> "17. It would seem straightforward that if no information is held, a reply confirming the non-existence of information could be provided without fear of likely prejudice to security.
>
> 18. Unfortunately, such an approach would be likely to prejudice security as:
>
> - It discloses what the NZSIS does not know.
> - It leaves the NZSIS open to orchestrated requests designed to flush out specific areas of investigation.
>
> 19. There are two principal concerns associated with confirming that no information is held:
>
> - Not knowing whether the NZSIS is investigating a particular activity or not has something of a deterrent effect. If it becomes a simple exercise to identify what is not of interest to the NZSIS, the benefit of the deterrent effect is lost.

---

194 New Zealand Security Intelligence Service, 'NZSIS Response to Information Requests' <http://www.nzsis.govt.nz/contact/nzsis-response-to-information-requests/> accessed 14 December 2015.

195 New Zealand Security Intelligence Service, 'Application of s10 of the Official Information Act 1982 and s32 of the Privacy Act 1993 by the NZSIS' < http://www.nzsis.govt.nz/assets/media/Application-of-S10-of-the-OIA-1982-and-S32-of-the-PA-1993.docx> accessed 14 December 2015.

196 ibid paras 6–12.

- If a correspondent is undertaking activities of security concern, and receives a "no information held" response for a subject they believed should be under investigation, they now know they have not been detected.

20. Unfortunately, the NZSIS is a natural target for orchestrated requests by some persons of security concern or their associates who want to understand more about the NZSIS' specific areas of investigation.

21. The only way to ensure that there is no prejudice to security is to be consistent in responses between these two groups (i.e. subjects of interest and subjects of no interest), and to issue a "neither confirm nor deny" response for both."

It is then noted that while the NCND response may cause concerns as to whether the rights of individuals are being protected, safeguards exist in the form of oversight by the Inspector-General of Intelligence and Security, political oversight and reviews by the Privacy Commissioner and Ombudsmen.[197]

Department of Labour policy

The Department of Labour's policy for handling official information requests also refers to the availability of a NCND response under s 10 of the OIA.[198] It states:[199]

> "This reason for refusal is used extremely rarely and in the Department may only be used if the Chief Executive or a direct report of the Chief Executive agrees. Legal advice is necessary."

Law Commission reports

The New Zealand Law Commission reviewed the OIA in 1997.[200] At that time, it noted that s 10 of the OIA had been applied to documents in only one case in 1988, which involved a request for information about CAZAB intelligence conferences attended by New Zealand representatives, following the release of Peter Wright's book *Spycatcher*.[201] The NZSIS used the NCND response in relation to the information requested. On review, the Chief Ombudsman accepted the Director of Security's reliance on s 10. His case note in *Case No. 1387* sets out that:[202]

---

197 ibid para 23.
198 Department of Labour, *Policy for handling Official Information Requests* (2009).
199 ibid 43.
200 Law Commission, *Review of the Official Information Act 1982* (NZLC, R40, October 1997).
201 ibid para 264.
202 (1989) *Ninth Compendium of Case Notes of the Ombudsmen* 102.

The concern was to avoid releasing material about New Zealand's liaison arrangement with overseas intelligence services. Sir Guy Powles as Chief Ombudsman in his 1976 report on the Service had stated that, in general, "it would not be proper to make any public comment" on the relationship between the Service and its overseas counterparts.

Under s 4 of the New Zealand Security Intelligence Service Act 1969, one of the functions of the Service is to communicate intelligence to such persons and in such manner as the Director considers to be in the interests of security, so the Chief Ombudsman must "to a great extent accept the judgment of the Director of Security in such matters".

Referring to *Commissioner of Police v Ombudsman*,[203] the words "would be likely" in ss 6 and 10 of the OIA do not set a high threshold and mean no more than "a distinct or significant possibility" that the prejudicial result would occur.

The reasons for withholding information under s 6 were conclusive; there was no element of countervailing argument as under s 9.

The Law Commission then observed that ss 6, 7 and 10 of the OIA "protect the international relations of New Zealand, and the flow of information from other governments or international organisations" which "are about continuing relationships with others, some of which are of major importance to New Zealand's vital interests".[204] It noted that judging the likely prejudice was a difficult task and would frequently involve intangible considerations. It did not recommend any change to those provisions.[205]

The most recent review of the OIA was completed in 2012.[206] Section 10 of the OIA was not discussed, and no issues were raised with the operation of ss 6, 7 or 9(2)(b) in relation to s 10.

The Privacy Act was also reviewed in 2011.[207] In its submission to the Law Commission, the NZSIS explained the circumstances in which it relied on the NCND response (as set out at paras 66 and 67 above). It noted that it was using the NCND response more broadly than it would wish because of the concern about orchestrated requests – that if one person receives a "no information held" request and another receives a NCND response, if this information was shared between them, it would indicate that the second person was of interest while the first was not.[208] The Law Commission observed that there had been a large increase in the number of access request received by the NZSIS in 2009 compared to the years before, probably because of media publicity about politicians and political activists.

---

[203] [1985] 1 NZLR 578 (HC); aff'd by the Court of Appeal [1988] NZLR 385.
[204] Law Commission (n 200), para 276.
[205] ibid para 277.
[206] Law Commission, *The Public's Right to Know: Review of the Official Information Legislation* (NZLC, R125, June 2012).
[207] Law Commission, *Review of the Privacy Act 1993: Review of the Law of Privacy Stage 4* (NZLC, R123, June 2011).
[208] ibid para 4.85.

In light of this broader use of the NCND principle, the NZSIS proposed a partial exemption from the access principle altogether. It envisaged that this exemption relate to intelligence investigatory material held by intelligence organisations (as opposed to material relating to security generally), and could be limited to material created within a particular period. The NZSIS acknowledged that any such exemption would need to be accompanied by robust accountability mechanisms, such as annual reporting and powers for the Privacy Commissioner to review the application of the exemption.[209]

The Law Commission considered that proposal best addressed through an upcoming review of intelligence and security organisations because it involved a significant change to the existing provisions and required submissions from other interested parties. It observed that the NZSIS could continue to use the NCND response under s 32 in the meantime, noting that the NZSIS's use of s 32 has been supported in a recent Privacy Commissioner case note.[210]

In that case note, *Case Note 219773*, from 2010,[211] the Commissioner upheld the NZSIS's reliance on s 32 in its response to the requester, and stated:

> "Section 32 enables the Service to uphold the integrity of its intelligence gathering function, which relies on discretion and the keeping of confidences. Section 32 allows that work to continue by allowing the Service to be consistent in responses to both subjects of interest and subjects of no interest when requests for information are made to it.
>
> This consistent response reduces the Service's susceptibility to orchestrated requests for information and any prejudice to security by disclosing what the Service does and does not know. This fits with the prospective nature of the Service's investigations and its need to preserve its position."

The independent review of the intelligence and security agencies and their governing legislation that the Law Commission referred to is a periodic review required under s 21 of the Intelligence and Security Committee Act 1996, which aims to increase the level of Parliamentary oversight and review of intelligence and security agencies.[212] This is currently ongoing, with consultation having run from 6 July to 14 August 2015 and a report expected by 29 February 2016.[213] The terms of reference state that one of the areas the reviewers will take into account is the Law Commission's work on whether

---

[209] ibid.
[210] ibid para 4.86.
[211] [2010] NZ PrivCmr 25 (An Individual Requests Personal Information from the New Zealand Security Intelligence Service).
[212] Long title to the Intelligence and Security Committee Act 1996.
[213] Ministry of Justice, 'Independent Review of Intelligence and Security' <https://consultations.justice.govt.nz/independent/iris/> accessed 10 January 2016.

current court processes are sufficient for dealing with classified and security sensitive information.[214]

Conclusion on statutory framework for information requests

In practice, it appears that the NCND response to information requests is used predominantly by the NZSIS, but it is used more frequently than the "very limited circumstances" referred to in the Privacy Commissioner's website. There does not appear to be much resistance or challenge to the way the NCND response is currently used in this context.

What accountability bodies outside of the courts have discussed NCND?

We have not been able to locate any discussion of NCND by accountability bodies outside of the courts, Privacy Commissioner or Ombudsman.

Is there any judicial treatment or discussion of NCND?

The two case notes discussed above in the Law Commission reports (*Case No. 1387* from the Chief Ombudsman and *Case Note 219773* from the Privacy Commissioner) discuss the NZSIS's use of the NCND response in the most detail. Other examples of the NCND response to information requests having been used in different contexts include:

Man seeks information from Police (Case Note 202975).[215] The Police refused to confirm or deny whether they held surveillance information on a requester. The Commissioner stated:

> "I accepted that in some circumstances confirming that someone has not been under surveillance could be highly relevant to the Police's ability to maintain the law, and could potentially be withheld under section 32. However, I was not satisfied that this was the case here. This was because the Police did not provide any evidence as to why the complainant would be likely to commit offences in the future if he knew that he had not been under surveillance in the past."

Case Note W39937.[216] In a prosecution relating to fisheries legislation, the requester sought from the Minister of Fisheries the file of the person he alleged was an informant. The Minister declined to confirm the existence or non-existence of such a file, relying on the maintenance of the law ground for withholding information. The Ombudsman highlighted the reliance on informants in criminal investigations and the public interest in protecting the identity of informants, and said:

---

[214] Ministry of Justice, 'Intelligence and security agencies review - Terms of reference' <http://www.justice. govt.nz/publications/global-publications/i/intelligence-and-security-agencies-review> accessed 10 January 2016.
[215] [2010] NZPrivCmr 19.
[216] (2000) *12th Compendium of Case Notes of the Ombudsmen* 82.

> As noted above, any disclosure that a person is or has been an informant for a law enforcement agency is likely to prejudice the interest protected by s 6(c) of the Official Information Act. However, a denial that a named person is or was an informant generally or in relation to a specific case is also likely to result in similar prejudice by reason of consequent deductions which may be made.
>
> The Ombudsman confirmed that it was appropriate for the Minister to rely on s 10 of the OIA because the interest protected by s 6(c) of the OIA would likely be prejudiced by the disclosure of the existence or non-existence of such information.

There does not appear to be any direct judicial discussion of NCND, and the only time it has been mentioned as obiter is in the public interest immunity context. In the cases *Choudry I*[217] and *Choudry II*,[218] one of the interlocutory issues related to a ministerial certificate provided that release of documents would prejudice national security. A slightly amended certificate was provided after the decision in *Choudry I*, and in *Choudry II* the majority held that it was unable to go behind the certificate as provided.

In *Choudry I*, the Court recognised that at times Parliament conferred an apparently conclusive power to prevent independent examination of an issue through the ability to neither confirm nor deny the existence of information (such as under s 10 of the OIA), but none of those provisions applied in that case, such that disclosure could be compelled.[219] In *Choudry II*, the Court again referred to the ability to provide a NCND response, and noted that while it was not relevant, "their existence and their particular focus do emphasise the special position in the law of certain national security interests".[220]

In his dissent, Thomas J considered that the ministerial certificate was still inadequate and immunity should not be granted. One of the reasons was his Honour's dissatisfaction with the "neither confirm nor deny" approach that the Solicitor-General appeared to take with the information sought to be withheld. His Honour said:[221]

> "I do not apprehend that such an expansive objective should lead automatically to the conclusion that national security is so vital that the fair and effective administration of justice is assumed to be incapable of outweighing it."

Nonetheless, the majority's treatment of the NCND provisions show an acceptance that such a stance is required in the context of national security, as enacted by Parliament.

---

[217] *Choudry v Attorney-General* [1999] 2 NZLR 582 (CA) [*Choudry I*].
[218] *Choudry v Attorney-General* [1999] 3 NZLR 399 (CA) [*Choudry II*].
[219] *Choudry I* (n 217) 595.
[220] *Choudry II* (n 218) [15].
[221] ibid [87].

Summary

(i) When (in relation to what subject matters) and by whom is NCND commonly deployed?

There does not appear to be any area in which the New Zealand government adopts a consistent and explicit NCND policy. In the few instances the NCND response has been used in the media, it has been in the surveillance context, in relation to informants or intelligence capabilities. There is a statutory framework providing for NCND responses to information requests, which has been predominantly used by the intelligence services (mainly the New Zealand Security Intelligence Service (NZSIS)).

(ii) What concerns have been raised over the use of NCND, if any, and by whom?

Generally, few concerns have been raised over the use of NCND in New Zealand, perhaps due to its low level of use. While it is not often used, there appears to be an acceptance, especially in the freedom of information area, that the NCND response will be necessary in some circumstances. The NZSIS has raised that it appears to be using the NCND response more broadly than it would wish, and has proposed introducing a partial exemption for the access principle altogether, which may be dealt with in an upcoming review of intelligence and security organisations. Nonetheless, the Privacy Commissioner has supported the NZSIS's use of the NCND response in such contexts.

(iii) What controls or oversight, if any, is there of the use of NCND policy? Or, what controls or oversight have been recommended, and by whom?

There does not appear to be any policy governing the New Zealand government's use of NCND when dealing with the media. In relation to the information request framework, the Privacy Commissioner, the GCSB and NZSIS have publicly set out their policies on how and when they would use the NCND response. Ex-post safeguards over the use of NCND responses in the statutory context exist in the form of the Inspector-General of Intelligence and Security, political oversight and reviews by the Privacy Commissioner and Ombudsmen.

ANNEX II

Appendix to report of February 2016:
OPBP Further Research on 'Neither Confirm Nor Deny'
(October 2017)

Oxford Pro Bono Publico originally completed comparative research on 'Neither Confirm Nor Deny' in June 2016. In mid-2017, JUSTICE sought to revisit the project. It asked for an update on whether there had been any significant developments pertaining to 'Neither Confirm Nor Deny' in the jurisdictions originally investigated. JUSTICE also asked for further research on three points:

- Whether jurisdictions other than the United States have guidance on what constitutes 'official acknowledgment' of information;
- Whether bad faith standards, or some sort of equivalent, apply in jurisdictions outside of the United States; and
- How the statutory review and appeals systems operates in Canada, in particular if there are closed proceedings – with JUSTICE being specifically interested in whether a party to litigation is made aware of a potential error of law.

This Appendix supplies that further research. It begins with a very brief update on the United States, without any reference to the three further points above. It then provides additional research on other jurisdictions: Europe (including some further background on the European Union), Australia, New Zealand, and Canada. The penultimate part is a section on Canada, which also addresses the third bullet point above. Some concluding remarks are then made.

1. The United States: relevant recent developments

An offshoot of the Black Lives Matter movement has brought a case against the New York Police Department (NYPD) for issuing a Glomar response to a request for information on how the NYPD monitors public protests under New York's Freedom of Information Law. The Appellate Division, First Department of the New York Supreme Court in June 2016 held that use of the Glomar response by public authorities in New York was permissible, citing precedent. (Matter of Hanig v State of N.Y. Dept. of Motor Vehs., 79 NY2d 106, 110 [1992]) An appeal was lodged in May 2017. The case has been reported in a few newspapers, and could potentially be interesting if the appeal is successful, but there is no immediate need to vary the report because the litigation is ongoing and the US section of the report focussed on federal law rather than state law.

2. European law

General review of any changes to European law since the original report

The original report refers to both Council of Europe and European Union Law under the heading of European law. The report does not seem to look in detail at European Union

law. This review will therefore look at both any changes that have occurred in Council of Europe jurisprudence, and European Union law more generally.

Council of Europe

Convention 205 on Access to Official Documents is still not in force.[222] The Convention will enter into force when it has been ratified by 10 States. Currently 9 States have ratified the Convention.[223] Several of the States which have ratified the Convention have derogated or included reservations from it.[224]

A parliamentary report by the Committee on Culture, Science, Education and the Media, *Parliamentary Scrutiny over Corruption: Parliamentary Cooperation with the Investigative Media*, says Convention 205 should be ratified as soon as possible.[225] The report also refers to investigative journalism as a 'public asset' and notes there should be cooperation between the government and journalists.[226] It recommends enacting laws which 'ensure the widest possible access to information.'[227]

The Joint Declaration by the United Nations Special Rapporteur on Freedom of Opinion and Expression, the OSCE Representative on Freedom of the Media and the OAS Special Rapporteur on *Freedom of Expression and Countering Violent Extremism* 2016 says, 'States and public officials should encourage open debate and access to information about all topics.'[228]

The 2017 report on *Freedom of Expression and Fake News, Disinformation and Propaganda* says 'State actors should, in accordance with their domestic and international legal obligations and their public duties, take care to ensure that they disseminate reliable and trustworthy information, including about matters of public interest, such as the economy, public health, security and the environment.'[229]

The original OPBP report recognises that NCND policies may be seen as infringements of certain rights in the European Convention on Human Rights. Where there is found to be an infringement the infringing state must show that the interference complained of had been "necessary in a democratic society"[230].

In the recent case of *Magyar Helsinki Bizottsag v Hungary* the court held that

---

222 http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/205.

223 Ibid.

224 Ibid.

225 Doc 14274, 20th March 2017, http://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=23241&lang=en, at 7.1.1.

226 Ibid, at 3.

227 Ibid, at 6.1.

228 http://www.osce.org/fom/237966?download=true at 2(f)

229 Joint Declaration by the United Nations Special Rapporteur on Freedom of Opinion and Expression, the OSCE Representative on Freedom of the Media and the OAS Special Rapporteur http://www.osce.org/fom/302796?download=true at 2(d)

230 *Grand Chamber judgment Magyar Helsinki Bizottsag v Hungary* (Application no. 18030/11) on the right of access to information of a NGO (8th November 2016).

notwithstanding the discretion left to the respondent State (its "margin of appreciation"), there had not been a reasonable relationship of proportionality between the measure complained of (refusal to provide the names of the ex officio defence counsel and the number of times they had been appointed to act as counsel in certain jurisdictions) and the legitimate aim pursued (protection of the rights of others). Thus, where a Convention right can be seen to be infringed by an NCND response, the infringement must be shown to be justified with a legitimate aim, and proportionate.

It consequently appears that there have not been any significant updates since the draft report on the kind of evidence required to justify on NCND response. It instead appears that the focus is on ensuring States ratify Convention 205.

European Union Law

Article 42 of the Charter of Fundamental Rights of the European Union says, 'Any citizen of the Union, and any natural or legal person residing or having its registered office in a Member State, has a right of access to European Parliament, Council and Commission documents.'[231] Article 11 gives 'the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas'.[232]

According to Article 52(1) and (2) of the Charter of Fundamental Rights, any limitation on the exercise of the rights and freedoms recognised by that charter must be provided for by law and respect the essence of those rights and freedoms.[233] Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others. Rights recognised by the Charter for which provision is made in the Treaties are to be exercised under the conditions and within the limits defined by those Treaties.

These Charter rights are likely to be interpreted in a similar way to Article 10 ECHR.[234] However, in the case of *Thesing and Bloomberg Finance v ECB*, it was concluded that restricting the access to the documents did not breach the Charter because the facts differed from those in the European Court of Human Rights cases.[235]

A recent decision of the Court of Justice of the European Union put in place rules concerning public access to the documents held by it in the exercise of its administrative functions.[236] This held that applications for access to documents can be refused for reasons of public interest, as regards public security, defence and military matters, international

---

231 http://www.europarl.europa.eu/charter/pdf/text_en.pdf

232 Ibid.

233 Ibid.

234 T 590/10 *Thesing and Bloomberg Finance v ECB* (November 2012) at [72].

235 Ibid, at [76]–[80].

236 C 445/3 decision of 11th October 2016 concerning public access to documents held by the Court of Justice of the European Union in the exercise of its administrative functions, http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016D1130%2801%29&from=EN .

relations, or the financial, monetary or economic policy of the European Union or a Member State.[237] If the Court of Justice of the European Union is not in a position to grant access to the document requested, it shall, within the period laid down in paragraph 2 and in writing, inform the applicant of the reasons for the total or partial refusal and inform the applicant of his or her right to make a confirmatory application within 1 month of receipt of the reply.[238] In the event of a total or partial refusal of his or her initial application, the applicant may make a confirmatory application.[239] In the event that the Court of Justice of the European Union refuses, totally or partially, a confirmatory application, it shall inform the applicant of the remedies open to him or her to challenge that refusal, namely instituting court proceedings or making a complaint to the European Ombudsman, under the conditions laid down in Articles 263 and 228 of the Treaty on the Functioning of the European Union.[240]

There has also been found to be a principle of transparency 'in Articles 1 TEU and 10 TEU and in Article 15 TFEU. It enables citizens to participate more closely in the decision-making process and guarantees that the administration enjoys greater legitimacy and is more effective and more accountable to the citizen in a democratic system.'[241]

Thus, European Union law seems to use a similar test to ECHR law on whether a right to access information/receive information has been infringed, and whether this can be justified. However, this test may apply differently in practice. There are no specific standards for NCND policies.

Does the jurisdiction have guidance on what amounts to 'official acknowledgement' of information?

Council of Europe

There is no clear guidance on what amounts to 'official acknowledgement' of information, or what might constitute something akin to the official acknowledgment doctrine in the United States. Convention 205 states, however, that 'a request for access to an official document shall be dealt with by any public authority holding the document. If the public authority does not hold the requested official document or if it is not authorised to process that request, it shall, wherever possible, refer the application or the applicant to the competent public authority.'[242] This could be read as suggesting that the authority that deals with the request acknowledges that it has/is authorised to deal with requests for the information.

European Union law

---

237 Ibid, at Art 3(1)(a).
238 Ibid, at Art 5(3).
239 Ibid, at Art 6(1).
240 Ibid, at Art 7(2).
241 Joined Cases C-92/09 and C-93/09 *Volker und Markus Schecke GbR v Land Hessen* at [52]
242 Council of Europe Convention on Access to Documents, CETS no. 205, https://rm.coe.int/1680084826, at Art 5(2).

The Court decision discussed above on public access to documents says that the applicant must be sent a written receipt of the application being received.[243] It does not however require the authority to say whether or not they have the information.

Do bad faith standards, or some equivalent, apply in the jurisdiction?

Council of Europe

Convention 205 says that 'limitations shall be set down precisely in law, be necessary in a democratic society and be proportionate'[244] to set aims. It continues that 'access to information contained in an official document may be refused if its disclosure would or would be likely to harm any of the [set aims], unless there is an overriding public interest in disclosure'.[245] Bad faith standards are not therefore specified in the Convention, but there does seem to be a focus on limitations being used to achieve certain aims.

European Union Law

The C 445/3 decision of 11th October 2016, mentioned above, requires refusals of access to information on the grounds of public interest to occur where 'disclosure would undermine the protection of' public interest.[246] Thus, although bad faith standards are not mentioned, it seems that refusals of access to information must be to genuinely protect the public interest.

3. Australia: relevant recent developments and the position on bad faith

To recapitulate the general legal position: section 25 of the *Freedom of Information Act 1982* (at the Commonwealth level) provides:

> ***25*** **Information as to existence of certain documents**
> (1) Nothing in this Act shall be taken to require an agency or Minister to give information as to the existence or non-existence of a document where information as to the existence or non-existence of that document, if included in a document of an agency, would cause the last-mentioned document to be:
> (a) an exempt document by virtue of section 33 or subsection 37(1) or 45A(1); or
> (b) an exempt document to the extent referred to in subsection 45A(2) or (3).
> (2) If a request relates to a document that is, or if it existed would be, of a kind referred to in subsection (1), the agency or Minister dealing with the request may give notice in writing to the applicant that the agency or the Minister (as the case may be) neither confirms nor denies the existence, as a document of the agency or an official document of the Minister, of such a document but that, assuming the existence of such a document, it would be:
> (a) an exempt document by virtue of section 33 or subsection 37(1) or 45A(1); or
> (b) an exempt document to the extent referred to in subsection 45A(2) or (3).
> (3) If a notice is given under subsection (2) of this section:

[243] See n 15 above, at Art 5(1).
[244] See n 21 above, at Art 3(1).
[245] Ibid, at Art 3(2).
[246] See n 15 above, at Art 3(1).

(a) section 26 applies as if the decision to give the notice were a decision referred to in that section; and

(b) the decision is taken, for the purposes of Part VI, to be a decision refusing to grant access to the document in accordance with the request referred to in subsection (2) of this section, for the reason that the document would, if it existed, be:

(i) an exempt document by virtue of section 33 or subsection 37(1) or 45A(1); or

(ii) an exempt document to the extent referred to in subsection 45A(2) or (3).

Thus an agency to which, or a Minister to whom, the Act applies does not have to reveal whether a document exists or does not exist in certain circumstances. Broadly, they may respond to a request by neither confirming nor denying the existence of a document the disclosure of which would (or could reasonably be expected to) affect:

(a) national security, defence or international relations (s 33);
(b) enforcement of law or protection of public safety (s 37); or
(c) the role of the Parliamentary Budget Officer or Office (s 45A).

The Explanatory Memorandum to the Freedom of Information Bill 1981 (Cth) relevantly states on page 23:

> Clause 25 – Information as to existence of certain documents
>
> 72. Sub-clause 25(1) entitles an agency or Minister to withhold information as to the existence or non-existence of a document if disclosure of that information would be prejudicial to the public interest for a reason specified in sub-clause 33(1) or would affect law enforcement for a reason specified in sub-clause 37(1).
>
> 73. Sub-clause 25(2) deals with the case where a request is made for access to a document and the document is or, if it existed, would be of such a kind that information about its existence might be withheld under sub-clause 25(1). In such a case, the agency or Minister dealing with the request may notify the applicant that the existence of the document is neither confirmed nor denied but that, if the document existed, it would be an exempt document. Reasons for giving such a notice must be furnished in accordance with clause 26 …

Additionally, the Australian Information Commissioner issued guidelines pursuant to s 93A of the Act. Part 3, which deals with processing and deciding on requests for access, relevantly states:

> **Refusing to confirm or deny existence of a document**
>
> 3.93 The act of confirming or denying the existence of a document can sometimes cause damage similar to disclosing the document itself. For example, merely knowing that an agency has a current telecommunications interception warrant in connection with a specific telephone service would be sufficient warning to a suspect who could modify their behaviour and possibly undermine an investigation into serious criminal activity.
>
> 3.94 Section 25(2) allows an agency or minister to give an applicant notice in writing that does not confirm or deny the existence of a document but instead tells the applicant that, if it existed, such a document would be exempt. This option is only available in relation to the exemptions in ss 33 (documents affecting national security, defence or international relations), 37(1) (documents affecting enforcement of law and protection of public safety) and 45A (Parliamentary Budget Office documents). The other requirements of a s 26 notice still apply (see [3.145] below).
>
> 3.95 Agencies and ministers should use s 25 only in exceptional circumstances. …

Part 5 of the guidelines deals with exemptions, and further explains:

> **Refusal to confirm or deny existence of a document**
>
> 5.50 In some instances, the act of confirming or denying whether a document exists can cause harm. For example, knowing that an agency possesses a copy of a particular document, coupled with the knowledge that the document could originate from only one source, might disclose a confidential source resulting in the effective loss of important information.
>
> 5.51 Section 25 of the FOI Act provides that agencies do not need to give information about the existence of documents in another document, such as a s 26 notice, if including that information would cause the latter to be exempt on the grounds set out in ss 33, 37(1) or 45A. … The agency may instead give the applicant notice in writing that it neither confirms nor denies the existence of the document, but if the document existed, it would be exempt under ss 33, 37(1) or 45A.
>
> 5.52 As use of this section has the effect of refusing a request for access to a document without providing reasons, use of s 25 should be reserved strictly for cases where the content of the material requires it.

There has been some recent case law on NCND in Australia. In *Brooks and Secretary, Department of Defence (Freedom of information)* [2017] AATA 258 (14 February 2017), Deputy President J W Constance importantly held:

> 30. It is the fact of denial or confirmation of the existence of documents, if that confirmation or denial was itself recorded in a document, which must meet the requirements of section 33 to be an exempt document. If the requirements of section 33 are met in these circumstances, the agency or Minister is empowered to give the subject notice. At no stage of this process is the agency or Minister required to consider whether there are, in fact, documents which themselves are exempt under section 33. Furthermore, subsection 25(2) does not require that a "document" be assumed to exist and then be subjected to the requirements of section 33.
>
> 31. As Counsel for the Secretary correctly pointed out, the interpretation for which Ms Brooks argues would require a decision-maker to construct an imaginary document, including the information it may contain, and then determine whether this hypothetical document would be exempt under section 33. I do not accept that this was the intention of Parliament.

In reaching this decision, the Deputy President in *Brooks* rejected the Tribunal's decision in *iNova Pharmaceuticals (Australia) Pty Ltd and Secretary, Department of Health and Ageing* [2010] AATA 542.[247] The Deputy President noted that that case had been appealed to the Federal Court,[248] where Emmett J relevantly held: 'Where s 25 is invoked, the agency has no obligation to make any attempt to identify documents that fall within the relevant request. Rather, a response of the kind contemplated by s 25 can be made solely on the basis of the form of the request.'[249]

The Deputy President in *Brooks* also considered the decision in *Department of Community Services v Jephcott* (1985) 8 FCR 85, and acknowledged that Davies J expressed a contrary

---

247 *Brooks and Secretary, Department of Defence (Freedom of information)* [2017] AATA 258 (14 February 2017), [32].

248 Ibid [33].

249 *Secretary, Department of Health and Ageing v iNova Pharmaceuticals (Australia) Pty Ltd* (2010) 191 FCR 573, [8].

view.[250] However, the Deputy President held that the judgment of Forster J is to be preferred, and noted that '[t]he third member of the Full Court did not consider the point.'[251]

The Deputy President also drew support from the Explanatory Memorandum, concluding 'that an enquiry into the nature of a document itself, or a hypothetical document, is not required.'[252]

You asked specifically about the position on 'good faith' or 'bad faith'.

Section 54W(a)(i) of the *Freedom of Information Act 1982* (Cth) provides that '[t]he Information Commissioner may decide not to undertake an IC review, or not to continue to undertake an IC review, if … [he or she] is satisfied [that] … the IC review application is frivolous, vexatious, misconceived, lacking in substance or not made in good faith'. The Information Commissioner may likewise decide not to investigate a complaint into an agency's action if he or she is satisfied 'that the complaint is frivolous, vexatious, misconceived, lacking in substance or not made in good faith': s 73(e).

There are similar provisions in Victoria: *Freedom of Information Act 1982* (Vic), ss 49G(1)(a) and 61B(2)(c). However, these do not relate to good or bad faith on the part of public authorities.

There are also provisions protecting people and entities from liability if they disclose information or make a complaint or perform a function in good faith: *Freedom of Information Act 1982* (Cth), ss 55Z, 85, 89E, 90, 92. There are similar provisions which require 'good faith' in other Australian jurisdictions:

(a) *Freedom of Information Act 1982* (Vic), s 63B;
(b) *Freedom of Information Act 1992* (WA), ss 80, 104, 105, 106;
(c) *Information Act 2002* (NT), s 151; and
(d) *Government Information (Public Access) Act 2009* (NSW), ss 113, 114, 115.

The *Freedom of Information Act 2016* (ACT) will commence on 1 January 2018.[253] Schedule 2 of that Act lists factors that favour disclosure in the public interest. One of the factors specified (in s 2.1(a)(vi)) is if 'disclosure of the information could reasonably be expected to … reveal or substantiate that an agency or public official had engaged in misconduct or negligent, improper or unlawful conduct or has acted maliciously or in bad faith'.

In *Sternberg v Blue Mountains City Council* [2017] NSWCATAD 67 (3 March 2017), Senior Member Dr J Lucy affirmed a council's decision in respect of an access application under the

---

250 *Brooks and Secretary, Department of Defence (Freedom of information)* [2017] AATA 258 (14 February 2017), [34].
251 Ibid [36]. See also [35].
252 Ibid [38]. See also [37].
253 *Justice and Community Safety Legislation Amendment Act 2017 (No 2)*, s 19.

Government Information (Public Access) Act 2009 (NSW). The council had refuse to confirm or deny that the requested information was held by it.

The Senior Member in *Sternberg* relevantly held as follows in relation to bad faith:

> 43. The applicant submits, relying upon *Fahey v NSW Office of Liquor, Gaming and Racing* [2012] NSWADT 181 at [30] and [73], that there is a public interest consideration in disclosing the identity of a complainant who makes false complaints. He says that that the complaint contained in the Letter to Council was not made in good faith. The applicant refers to a published Council document which states that Council will not disclose the name, address or other personal information of members of the community who report, in good faith, information to the Council relating to the actions of others who have acted contrary to laws and regulations.
> 44. In support of the applicant's submission that the complaint was not made in good faith, he submits:
>
> (1) Council had advised Mr and Mrs Neighbour that neither the applicant's driveway nor the planting of trees on the nature strip contravened any regulations;
> (2) The placement of the applicant's letterbox complied with Australia Post's requirements, as it was positioned at the junction of the driveway with the road;
> (3) The applicant and his wife had never placed "Do not park here" signs in front of their property during the Leura Garden Festival, as claimed in the Letter to Council. Rather, the festival organisers placed them there. The claim in the Letter to Council that the author of the letter had seen the applicant or his wife place the signs in front of their property was accordingly a lie;
> (4) The request in the Letter to Council that the applicant and his wife remove plants on the nature strip and move their letterbox, "consistent with everyone else" was a malicious statement. This was because many other properties on the street had letterboxes and trees on the nature strip, some of which blocked pedestrian access and, contrary to the writer's claim, pedestrians did not have to step on to the road when walking in front of the applicant's property;
> (5) The Neighbours had a letterbox on the nature reserve and pedestrian thoroughfare was blocked by a garden bed between their property boundary and the roadway.
>
> 45. The applicant's allegations of bad faith depend in part upon his unproven assumption that Mr Neighbour is the author of the Letter to Council. To the extent that he relies upon the observation in the letter that the author saw the applicant and his wife place "do not park here" signs outside the property, it is possible that the author was mistaken as to the identity of the person he saw placing the signs. There is insufficient evidence for the Tribunal to conclude that the author of the letter was lying. The Tribunal accepts the applicant's evidence that the placement of his letterbox complies with Australia Post's requirements. It also accepts photographic evidence that shows there is room for pedestrians to walk next to the plants on the applicant's nature strip. However, there is nothing to suggest that the author's claim that pedestrians do, in fact, step on to the road is not correct or, at the very least, reflects a belief genuinely held.
> 46. The Tribunal is not satisfied that the complaint is "false", nor that it was made in bad faith. The applicant accepts that he and his wife have planted trees and plants on the nature strip as alleged and also accepts that their letterbox is located where the author of the letter says it is located. The author of the letter makes a claim concerning the placement of signs which may be incorrect, but this could be due to a mistake. It appears, in any event, that the substance of the complaint is not about the signs but about the location of the plants and letterbox on the nature strip, and about whether the applicant and his wife have council permission for their driveway.

47. For these reasons, the Tribunal does not consider that, if there is a public interest consideration in favour of disclosing the identity of a complainant who makes false complaints, or makes complaints in bad faith, such a consideration applies in these proceedings.

4. New Zealand

Updates

Case Note 284416

There has been one further decision of the New Zealand Privacy Commissioner pertaining to 'neither confirm nor deny', on 31 May 2017. This is noted in Case Note 284416 [2017] NZPrivCmr 5.[254] A man had asked for any file and/or information held in relation to him by the New Zealand Security Intelligence Service ('the SIS') and the Government Communications Security Bureau ('the GCSB'). The SIS and the GCSB issued a 'neither confirm nor deny' response, invoking the security or defence of New Zealand mentioned in s 27(1)(a) of the Privacy Act 1993.

The man took a claim to the Privacy Commissioner. He noted that he had asked under the Official Information Act about the proportion of 'neither confirm nor deny' responses – s 32 responses – given to requests like his. The GCSB had said that from October 2014 to October 2016, 88% of requests under the Act ha d been given a 'neither confirm nor deny' responses. The SIS said that in the last six months (it claimed it did not keep statistics going further back than six months) a 'neither confirm nor deny' response had been in 50% of cases. The man raised a challenge relating to principle 6 of the Privacy Act, which says that where an agency holds readily retrievable personal information, the individual is entitled to obtain confirmation that the agency holds the information and to have access to that information. The Commissioner observed that principle 6 is subject to s 32 of the Act, which allows the SIS to neither confirm nor deny the existence of information about a person. The Commissioner stated:[255]

> Because of security considerations, the Service and the Bureau cannot be as open with individuals about the personal information they hold or don't hold about them, compared to other public sector agencies. Due to the sensitive nature of their work, responding to principle 6 requests and revealing what is known or not known about a person can have national security implications. Individuals could share principle 6 responses with each other to draw inferences about what the Service or the Bureau is or is not aware of. A requester may in fact present no security risk, however section 32 allows the Service and the Bureau to take a cautious approach to revealing whether or not it holds the personal information requested.

The Commissioner observed that it had asked the SIS and GCSB to provide comments. The SIS had said that it disclosed information unless there was good reason to refuse, or to

[254] Available online at http://www.nzlii.org/cgi-bin/sinodisp/nz/cases/NZPrivCmr/2017/5.html?query=%22neither%20confirm%20nor%20deny%22 (last accessed 14 October 2017).
[255] Ibid.

give a notice neither confirming nor denying the existence of the information. It had said that a "case by case" approach was used. The GCSB said the same: that it had reasons for invoking neither confirm nor deny in this case, and that it considered information requests on a case by case basis. The Privacy Commissioner accepted this reasoning and "concluded … that the complainant had not suffered an interference with his privacy." The Privacy Commissioner noted that the complainant was unhappy with the outcome, but acknowledged that the complainant could prepare a case note. The Commissioner observed that, "It can be unsettling for people to receive a 'neither confirm not [sic] deny' response … However, in cases such as these … a complainant can take some comfort from the fact the decisions of the Service and Bureau have been independently reviewed by the Privacy Commissioner and found not to be contrary to the Privacy Act." It was not clear, however, the extent to which the Privacy Commissioner was able to inspect the bases of these decisions.

Interestingly, the Commissioner added:

> … in general a requester is entitled to ask for and receive any personal information held by an agency, without having to disclose why the information is being requested. However, an information request to the Service or the Bureau will involve an additional assessment of security implications of the response. Giving context information for the request may, in specific cases, allow the Service or Bureau to provide a factual response, rather than relying on section 32 to neither confirm nor deny whether information exists.

The upshot of this comment is that the provision of "context[ual] information" may allow a more direct ("factual") response from the relevant authorities.

Further political use of NCND

It is worth noting a US instance of use of 'neither confirm nor deny' with some impact on New Zealand. New Zealand has a longstanding legislated position of being nuclear-free (since 1987): that is, not allowing ships and other vessels carrying any nuclear material to dock in New Zealand ports. In mid-2016, in discussions about a US ship visit to New Zealand, US officials indicated that they would maintain their position of neither confirming nor denying the existence of nuclear weapons on ships going to New Zealand. However, New Zealand officials noted that they would still be able to satisfy themselves that ships were nuclear-free.[256]

Official acknowledgment

New Zealand does not appear to have a developed doctrine of the kind akin to the 'official acknowledgment' doctrine in the United States, which indicates that past disclosure of

[256] Vernon Small, 'No Confirm or Deny Required from US for Ship Visit', says McCully', *Stuff Politics*, 12 June 2016, available online at http://www.stuff.co.nz/national/politics/80975944/No-confirm-or-deny-required-from-US-for-ship-visit-says-McCully (last accessed 14 October 2017).

information of the same kind means that the information is in the public domain and cannot be subject to a 'neither confirm nor deny' response.

What constitutes 'bad faith' or equivalent?

As the initial report noted, there is very little case law on 'neither confirm nor deny' – and, unsurprisingly, there has been no development of some 'bad faith' exception to the use of 'neither confirm nor deny'. No statutory regime refers to the unavailability of 'neither confirm nor deny' in instances where there has been bad faith.

5. Canada

Have there been any updates since the draft report on the kind of evidence required to justify an NCND response?

While "NCND" responses are used in a variety of contexts in Canada, there does not appear to be an overarching policy by the Federal Government, or any publicly available guidance, for when this response may be given. I have not found any new available policies or guidelines by the Federal Government on this issue.

Does Canada offer have guidance on what amounts to 'official acknowledgement' of information?

This question concerns the regime by which the Canadian government controls how people may make requests from the government and public bodies for information.

The Federal Government regulates the flow of government information, by request, through an access to information regime. The cornerstone federal legislation of this regime is the *Access to Information Act*.[257] This Act sets out who may request information from the government, which information can be requested, as well as when information may be refused, and how such refusals may be challenged.

Briefly, the Act provides to broad access to information to government information. Under section 4, this Act grants the right to every Canadian citizen or permanent resident to be given access to any record under the control of a government institution.[258] This right is limited by certain exemptions. These exemptions, set out by the Act (sections 13-26), are situations wherein the responsibilities of the Government require the head of a government institution to refuse to disclose a record. These situations are wide-ranging and include, for example, refusal to access a record where the record requested: contains information the disclosure of which could reasonably be expected to be injurious to, *inter alia*, the defence of

[257] *Access to Information Act*, (RSC, 1985 C. A-1). This Act was last amended 22 June 2017. Please note there are also equivalent provincial regimes.
[258] The terms "government institution" and "record" are defined by s. 3 of the Act.

Canada (s 15) contains personal information as defined by the *Privacy Act* (s. 19); contains information is to be published within a ninety-day period of the request (s. 26).

Where access to a record is refused, the head of the government institution who refuses access shall state either that (a) the record does not exist, or (b) the specific provision of the *Access to Information Act* on which the refusal was based, or "where the head of the institution does not indicate whether a record exists, the provision on which a refusal could reasonably be expected to be based if the record existed (s. 10)." The head of a government institution *may*, but is not required, to indicate whether a record exists (s. 10). Thus, essentially a "NCND" response can be given in response to the request for a government record. This does not preclude, however, the requirement for the head of the government institution to state the provision that would justify a refusal of access if the record did exist. Nor does this response preclude the right to the person who made the request to make a complaint to the Information Commissioner regarding the refusal.

Moreover, the Act sets out the avenue under which the Federal Court may review a refusal. Under s. 41 of the Act, any person who has been refused access to a record requested under the Act may, if a complaint has been made to the Information Commissioner, apply to the Court for a review of the matter within forty-five days after the time the results of an investigation of the complaint by the Information Commissioner are reported. The Act also sets out rules regulating how a review by the Federal Court may take place.

No record may be withheld from the Court where an application for review has been brought under sections 41, 42 or 44 of the Act. The Act further provides for receiving representations *ex parte* and conducting hearings *in camera* to avoid disclosure by the Court or any person of either: (a) the information or other material on the basis of which the head of a government institution would be authorized to refuse to disclose a part of the record requested under the Act; or (b) any information as to whether a record exists where the head of a government institution, in refusing to disclose the record under this Act, does not indicate whether it exists (see section 47).

Canada-specific research: how does the statutory review and appeals system in Canada operate if there are closed proceedings? Is the party to litigation made aware of a potential error of law?

As set out above, where a refusal is made to access a record under the access to information regime (even without a proceeding), a party is permitted to make a complaint about this refusal. Similarly, a review by the Federal Court may be undertaken and the hearing may be conducted *in camera* and representations may be received *ex parte*. My understanding is that these mechanisms would result in a hearing similar to a "closed proceeding."

The *Access to Information Act* does not stipulate the manner in which a response by the Information Commissioner or the Federal Court must be given. However, there is a body of Canadian administrative law that sets out principles by which decisions must be given.

For instance, in *Baker v Canada (Minister of Citizenship and Immigration)*, [1999] 2 SCR 817, the Supreme Court of Canada discusses the duty of procedural fairness, and how this duty at times will require a written explanation for a reason. This line of cases sets out the parameters and nature of this duty.[259] My preliminary research suggests these standards, at least presumptively, would apply in this context.

There are other areas of Canadian law where a hearing analogous to a "closed proceeding" may occur, for example the Security Certificate context – an immigration proceeding under the *Immigration and Refugee Protection Act (IRPA)* for the purpose of removing non-Canadians from Canada that are inadmissible for reasons of such as national security, violating human or international rights, or involvement in organized or serious crimes.[260] The security certificate regime has been subject to judicial scrutiny, notable in the Supreme Court of Canada's 2014 decision *Canada (Citizenship and Immigration) v Harkat*, 2014 SCC 37.[261]

Conclusion

There appear to be few significant political developments or decisions in these jurisdictions over the last year or so. The decision of the Privacy Commissioner in New Zealand does show increased concern with 'neither confirm nor deny' in the New Zealand context, and reveals an interesting attempt to draw attention to the regime – by asking agencies, through a freedom of information channel, to reveal the frequency of 'neither confirm nor deny' requests. The research has not revealed a developed 'official acknowledgment' doctrine of the kind that exists in the United States, nor a bad faith exception to the use of 'neither confirm nor deny'.

[259] See, for example: *Gray v Ontario (Director, Disability Support Program)* (2002), 212 DLR (4th) 353 (ONCA); *R v Sheppard*, 2002 SCC 26; *R v. Brown* (2002), 61 OR (3d) 619 (a few illustrations of the body of case law that discusses the duty to give reasons).

[260] See: Government of Canada, *Security certificates* 2015-12-01) https://www.publicsafety.gc.ca/cnt/ntnl-scrt/cntr-trrrsm/scrt-crtfcts-en.aspx.

[261] *Canada (Citizenship and Immigration) v. Harkat*, [2014] 2 SCR 33, 2014 SCC 37 (CanLII), <http://canlii.ca/t/g6v7s>, retrieved on 2017-08-28.