Law Commission Review of National Security Information in Proceedings

Thank you for inviting the Office of the Privacy Commissioner to make a submission on this review.

The review raises questions about the use of national security information in the context of civil and criminal proceedings, as well as administrative decisions and review under specific statutes such as the Immigration Act and the Telecommunications (Interception Capability and Security Act (TICSA). There are some linkages between the subject area of the review and the Privacy Commissioner's jurisdiction, and some related issues and concepts.

Broadly speaking, the review raises issues about a litigant's or applicant's access to information about them where relied on by public bodies which could have significant adverse impacts on the individual or their rights. This has direct parallels in the Privacy Commissioner's jurisdiction, and in our comments on chapter 2 of the Issues Paper, we note the importance of the right to access to information in our legal system.

An area of potential overlap is where a litigant or applicant makes an access request under the Privacy Act for personal information that is relevant to proceedings or an administrative decision. There is scope under the Privacy Act for an agency to refuse to release information in response to a request on national security grounds, including:[1]

- prejudice to the security or defence of New Zealand;
- prejudice to the international relations of the Government of New Zealand; or
- prejudice to the entrusting of confidential information to the Government of New Zealand by another government or international organisation.

The treatment of national security information in civil proceedings also has direct relevance to the resolution of Privacy Act information privacy requests involving national security information that come before the Human Rights Review Tribunal. Although access to information complaints involving the security and intelligence agencies cannot progress to the Tribunal,[2] complaints against other agencies such as the Police or Customs may do so.

Introductory comments – the Privacy Commissioner's jurisdiction

The Privacy Act has achieved a workable balance between access to information and the protection of national security interests and may provide some insights for designing a generic process for other contexts in which the rights of the individual must be balanced against the security interests of the state.

---

1 Privacy Act 1993, section 27(1)(a) and (b)

2 Privacy Act 1993, section 81.

Under the Privacy Act, an assertion of sensitivity on national security grounds does not automatically allow an agency to refuse to release information to a requester. The emphasis is on ensuring that an agency's decision not to release information is subject to an independent and confidential review. The material is reviewed using a risk-assessment approach to assess the likelihood of prejudice.

Briefly, the Privacy Act as it relates to national security information involves the following.

The Privacy Commissioner's role is to provide an independent review of agency decisions to refuse to release personal information to individual requesters on national security grounds (section 27(1)(a)). In order to investigate a complaint, the Privacy Commissioner may require the information in dispute to be produced for review.[3]

The Privacy Commissioner maintains strict secrecy (section 116). The secrecy provision provides an assurance that allows sensitive material to be reviewed, so that assertions of national security interests and other sensitivity grounds can be tested by the Privacy Commissioner as an independent statutory officer.

A national security certificate can be issued by the Prime Minister to preclude the Privacy Commissioner reviewing information where he or she considers that review may prejudice the security or defence of New Zealand or New Zealand's international relations.[4] Although this effectively "vetoes" the Privacy Commissioner's review and investigation, certain accountability mechanisms continue to operate:

- the Privacy Commissioner may make a public statement about the issue of a national security certificate;[5] provided that any such statement does not itself prejudice national security;[6]
- the Privacy Commissioner may make recommendations to an intelligence agency in relation to the investigation to the extent it has been carried out without reviewing the material;
- the requester may consider initiating judicial review proceedings in relation to the issue of the certificate; or
- the requester may initiate proceedings in the Tribunal, except where the agency involved is one of the intelligence agencies.

Once the Privacy Commissioner's investigation has been completed, the Commissioner may make a finding that particular information should be released to a requester. However the Commissioner has no power to order the release of that information. The issue is referred to the Human Rights Review Tribunal (except where the agency concerned is an intelligence agency), either via the Director of Human Rights Proceedings, or by the requester directly. It then becomes a matter for the Tribunal as a judicial body to make a substantive and enforceable order about whether the information sought should be released. In that case, the role of the Tribunal would fall within the scope of civil proceedings considered in chapter 5.

---

3 Privacy Act 1993, section 91(4), s 94(1A).
4 Privacy Act 1993, section 95(3)(a)
5 Privacy Act 1993, section 13
6 Privacy Act 1993, section 116(3). Cf Official Information Act 1982, section 31.

There is a specific process for access complaints involving the security and intelligence agencies. The jurisdiction of the Human Rights Review Tribunal is excluded for these complaints, and instead, the Privacy Commissioner can issue an opinion and recommendations on the matter to the agency concerned, and may subsequently raise the matter with the Prime Minister who must lay a copy of the Privacy Commissioner's report before Parliament.[7]

General comments – chapter 2

Significance of the right of access to personal information

We respectfully suggest that an individual's right of access to information about them, and to the reasons for decisions made about them, is another specific public policy interest that should be taken into account, in addition to the interests the Law Commission identifies in chapter 2.

As noted at para [1.24] the Privacy Act provides a right of access to personal information (principle 6). This is a foundational right which has been described by the Court of Appeal as being of "constitutional significance".[8] It is the one privacy principle that creates a legal and enforceable right as against public sector agencies.[9] It is also one of the two privacy principles where a breach amounts to an "interference with privacy" regardless of the level of harm sustained by the affected individual.[10]

Other privacy law parallels

Other relevant privacy principles are principle 7 (entitling a person to seek correction of information held about them) and principle 8 (requiring an agency to ensure that personal information is accurate, up to date, complete, relevant and not misleading before it is used by the agency for a particular purpose.

This has resonance with the principle of equality of arms principle discussed in chapter 2; in particular, the need for a person to be fully informed about the reasons for a decision affecting them or the basis for litigation involving them so that they can answer the Crown's case, the opportunity to seek to correct personal information that is inaccurate, and the opportunity to test the veracity of the information to ensure its accuracy.

Privacy law also emphasizes the principles of transparency, accountability, and the mitigation of adverse impacts on individuals through fair process, while balancing other important public interests such as national security.

---

7 Privacy Act 1993, s 81.

8 *Commissioner of Police v Ombudsman* [1988] 1NZLR 385. This decision predates the Privacy Act 1993, when the right of access was contained within the Official Information Act.

9 Privacy Act 1993, s 10(1).

10 The other principle is privacy principle 7 (the right of correction). Privacy Act, s 66(2).

Specific comments

Chapter 3 – Criminal proceedings

Q1 How should national security information be protected when used as grounds for a warrant?

We agree that suppression mechanisms could be explored if national security information is used as grounds for a warrant. The important principle is that sufficient information should be provided to the judicial officer, to be satisfied that the grounds for issuing the warrant have been met. Judicial officers are experienced in the handling of confidential, sensitive and privileged material, and should be trusted to deal appropriately with national security information. The issue is essentially one of process in protecting the information throughout the judicial process. Practical options might include showing the material to the judicial officer, discussing the material orally, and redacting any material held on the court file.[11]

The party supporting any suppression could have the opportunity to make arguments in favour of its continued application, should a challenge to the warrant eventuate. Any suppression applied should be reviewable by the judicial officer hearing any challenge to the warrant, or the judicial officer who issued the warrant.

Q2 Should there be a role for special advocates in a pre-trial hearing on disclosure under the Criminal Disclosure Act 2008

We agree that a process for independent review of material that is withheld from pre-trial disclosure under the Criminal Disclosure Act 2008 is desirable. Although section 30 of the Criminal Disclosure Act allows a defendant to apply for a disclosure order in relation to information that has been withheld, as identified, where the defendant has not been privy to the information, it may be difficult to satisfy the court that the public interest favours disclosure.

We are not persuaded that the initial disclosure question would necessarily need to involve special advocates. This function could be assigned to a statutory officer to provide a level of assurance to the defendant, the court and the public that reliance on national security grounds by the State to exclude relevant evidence has been independently assessed. This model might provide consistency of approach.

The role of a statutory reviewer could include examining the strength of the national security interest, and providing a view on the appropriate balancing of the public interest in the circumstances. This could assist the court to reach a view on the appropriate balancing where, as noted, there is little case law to provide guidance. It would also provide defendants with an automatic independent review procedure where national security grounds are relied on to limit disclosure.[12]

---

11 See, for example, the options in the Privacy Act, s 42, for furnishing information.

12 Although the information might be requested under the Privacy Act 1993, the Criminal Disclosure Act regime operates as a refusal ground by virtue of section 29(1)(ia).

One option might be to consider creating a review role within the Office of the Inspector-General of Intelligence and Security, to assess reliance on the national security withholding grounds by the intelligence agencies. A review might result in a recommendation to the agency concerned, with a copy to the judicial officer presiding over the proceeding. The review would be advisory, with the court having ultimate discretion about whether to make a disclosure order.

In relation to other agencies seeking to rely on national security grounds, one option could be to expand the role of the Privacy Commissioner to carry out the independent review. Although the test to be applied for criminal disclosure would be different to the Privacy Act test, there is substantial commonality with access to information cases.

Q3 Do sections 69 and 70 of the Evidence Act 2006 provide sufficient guidance to a trial judge in determining whether to exclude national security information?

The current mechanism provides for balancing interests in tension through judicial discretion to exclude evidence that is sensitive for reasons of confidentiality or security. This may affect the State's case, but in unusual circumstances it may also affect the defence case should the State object to the defendant's application to admit sensitive evidence. In our view, judges are the appropriate arbiters of whether sensitive information should be admitted and will be cognisant of the ramifications for each party of a decision to exclude evidence.

One reform option might be to develop a list of matters to be taken into account under section 70, along the lines of section 69(3), should additional guidance be considered necessary.

Q4 Should undercover security agents be able to use the same protections currently available to undercover Police officers, and give evidence anonymously?

We note the limitation in section 13A of the New Zealand Security Intelligence Service Act on publicly identifying a member of the Service but this restriction does not necessarily preclude members of the Service from giving evidence in a proceeding in the usual way, subject to appropriate publication restrictions.

If however the circumstances support protecting the identity of a security agent (in order to protect national security interests) then provision could be made for evidence to be given on an anonymous basis provided that there is sufficient judicial oversight to guard against any risk of abuse of process.[13]

[13] See Jonathan Carson "Judge critical of Police after botched Red Devils gang operation" Nelson Mail (13 June 2015) http://www.stuff.co.nz/nelson-mail/69299045/judge-critical-of-police-after-botched-red-devils-gang-operation

Q5 Does the Evidence Act 2006 provide sound mechanisms for national security information to be used in a criminal trial in a controlled way that protects against risks associated with full disclosure, while still allowing for it to be properly tested, given the primacy that should be afforded to fair trial rights?

As noted, there are measures available to protect sensitive evidence that is admitted. One option might be to develop a protocol that judges could refer to in considering options for the protection of national security information.

It may also be worth considering the option of codifying the common law that limits the use of documents disclosed through the discovery process to the particular proceeding, and restricts any collateral use.[14]

Q6 Do the current provisions allowing suppression orders provide for proper balancing of national security interests on the one hand and open justice on the other?

No comment.

Q7 Is there a need to make explicit the expectation that criminal proceedings will be discontinued if there is no other way to protect national security evidence and avoid prejudice to the accused, for example, through giving the judge the power to order that proceedings be dismissed rather than information disclosed?

We agree it would be desirable to make this judicial power explicit, in the interests of mitigating prejudice to the accused, in situations where it is not possible to achieve an appropriate balance of the competing interests.

Q8 Are any further mechanisms, or any expansion of existing mechanisms, needed to enable national security information to be used as evidence in criminal trials, including for terrorist acts?

No comment.

Chapter 4 – Administrative decisions and review

Q9 Should elements of administrative decision making processes involving national security information be standardised at the initial decision making stage?

We support consideration of a standardised process or standardised process features that offer the greatest protection for fundamental rights. In our view, a standardised process would best reflect and balance the various public interests involved, and is preferable to introducing variant approaches for each statutory regime or new context in which national security information can be relevant to decision makers.

A standard process is more likely to achieve the optimal balance between the interests in tension as a process designed in a specific context may be unduly influenced by the

---

[14] See also High Court Rules [8.30].

particular policy objectives of that regime. Any departure from the standard regime should be sufficiently and transparently justified on clear policy grounds.

A standard process also has the advantage that learnings and precedents can be applied in a range of factual circumstances. Over time a standard process would assume greater familiarity for decision makers, and for the Courts.

Q10 Should there be a single framework that applies to all reviews or appeals of administrative decisions that involve national security information?

We support a single framework for reviews or appeals, on the basis that standardisation of process is desirable for the reasons outlined above.

Q11 What features should such a single framework provide for? Should it involve special advocates, summaries of national security information or any other mechanisms to help ensure a fair hearing?

As noted above, a single framework needs to afford the greatest possible protection for fundamental rights. Any departure from the usual safeguards and protections needs to have clear thresholds and criteria.

It may be appropriate to include features such as special advocates and summaries of information where these are the best available options. We comment on the role of special advocates at Q 20-21.

The use of summaries might be appropriate in particular cases, provided that:

- there is a clear statutory basis and decision-making process for deciding to exercise that option, over providing the information in full; and
- there is provision for independent review of the summary against the substantive information (whether by the court or Tribunal or by an independent reviewer), and an ability to challenge or amend the summary where it is deficient.

Q12 Should courts or tribunals reviewing administrative decisions be able to consider information that has not been disclosed to the parties to the case?

Where undisclosed information has been instrumental in the decision affecting the individual, it would be necessary for the court or tribunal to be able to consider that information, using protective mechanisms as necessary. As part of its review, there should be scope for the review body to revisit the non-disclosure issue and issue a disclosure order as appropriate, for example requiring a summary of the information to be provided.

Chapter 5 – Civil proceedings

Q13 Should the courts be able to consider national security information that has not been disclosed to one of the parties to a claim in civil proceedings?

The presumption of “open justice” means that any form of closed proceedings should be used only on an exceptional basis.

The evidential criteria of relevance suggests that the courts should be able to consider national security information. However, if the information is not disclosed to both parties, adequate safeguards need to be in place to protect fairness.

Q14 Should New Zealand adopt a single overarching framework that applies to all civil proceedings?

We support the aim of developing a single framework that promotes consistency and a principled approach. However, we suggest that an element of judicial discretion should be included in the framework to ensure the fairness of any particular proceedings.

We also recommend that the framework incorporate "degrees of openness", so that a court can select the most open process that is appropriate in the circumstances, based on considerations such as the sensitivity of the information, the significance of the particular proceedings and the potential impact on the party the information relates to.

As a presumption, the more significant the potential impact of the information, the greater the need will be for process safeguards if restrictions are applied. We therefore support the suggested range of pathways in para 6.97, based on facilitating the optimal degree of disclosure and openness depending on the balance of interests at stake.

Q15 What features should such a process have? Should the process use special advocates, security-cleared lawyers, summaries of the national security information, or other mechanisms to ensure the interests of the non-Crown party are represented?

The process should have a range of options that reflect varying degrees of openness so that the court can select the appropriate procedure in the circumstances.[15] Ideally, the procedure selected would depend on an impact assessment, i.e. weighing up the potential impact on the affected party and the potential risk to national security interests. One feature that should be included is the right to challenge the procedure selected on fairness grounds.

In relation to the use of summaries, see our comments at Q11. In relation to the use of special advocates, see our comments at Q20-21.

It is worth noting the use of closed proceedings or "in caucus" proceedings in other civil proceeding contexts. See for example the judicial review proceedings, *Alpine Energy v Human Rights Review Tribunal*[16] where the respondent in an age discrimination case under the Human Rights Act sought review of the Tribunal's decision to order discovery of confidential material.

The High Court found that the Tribunal had made an error:[17]

---

15 For example, the spectrum of options between affording full natural justice rights and affording full protection of national security information identified on page 68 of the Issues Paper, could provide a range of options that apply in different circumstances, depending on the different weightings of the interests involved.

16 [2014] NZHC 2792, Gendall J.

17 At para [29], [31].

> *That error was simply that it adjudicated upon admissibility without appraising itself of the precise nature and content of the documents over which it was sitting as arbiter. As far as I can tell, none of the actual withheld and redacted documents were placed either before this Court or the Tribunal. This begs the question as to how it is possible to determine pivotal matters such as relevance and probative value in their absence… I am satisfied that a principled decision requires proper access to the evidence which is the subject matter of proceedings in order for a proper decision to be made.*

The Court concluded that the withheld and redacted documents should be provisionally admitted to the Tribunal "in caucus" to permit an informed decision on admissibility. The Court went on to suggest the option of having the evidence in the substantive hearing provided to the Tribunal, with the plaintiff being excluded to the extent that the evidence in question was traversed, but with an amicus to assist the Tribunal and the plaintiff in relation to review of and submissions on the material.[18]

Subsequently a closed hearing was held by the Tribunal, although the Tribunal did not have power to appoint assisting counsel, as suggested by the High Court.[19]

Ensuring there is flexibility to appoint assisting counsel across the courts and Tribunals who must weigh competing public interests such as national security is a feature that could usefully be considered. One issue is to how to appoint assisting counsel who have the appropriate clearance to review national security material without disclosing the fact of their clearance. This tension may be reduced where the review is conducted by a statutory officer, as discussed at Q2 above.

Chapter 6 – Reform – where to from here?

Q16 What types of security interests should be sufficient to displace the normal assumption that relevant information is disclosed to the affected parties? (In other words, how should we define national security for the purposes of this review?)

A generalised approach to defining "national security" can make it difficult to robustly verify that displacing the normal rights and assumptions is justified. We support a more granular approach to defining "national security" and articulating the public policy reasons for treating the information as particularly sensitive. It should be possible to identify with greater specificity the particular interests that require protection.

Some of these will be broadly operational for example, protecting operational methods or sources of information. Some will be specifically operational such as avoiding prejudice to ongoing inquiries or monitoring. Some will be diplomatic or economic, for example protecting international relations with another country through respecting confidentiality of shared information. Some will be mixed, for example protecting international information sharing arrangements in order to ensure ongoing reciprocal information sharing in the interests of New Zealand's intelligence collection.

---

18 At para [34].

19 *Waters v Alpine Energy Ltd (Discovery No. 2)* [2015] NZHRRT 7 (9 March 2015) at [9].

The advantage of a more granular approach is that it means that the various interests deserving protection can be organised in a hierarchy, so that there is greater clarity about the circumstances in which national security "trumps" other interests, and the circumstances in which it is one factor to be weighed in reaching an appropriate balancing of interests. As noted at para 6.97, not all risks to national security require the same level of protection.

A clearer definition of national security could also be useful in assessing the risk or threat to national security by any particular disclosure. It may also make it easier to make process decisions about when and how to depart from the usual presumptions of open justice and full disclosure to both parties and ensure that the appropriate compromise is selected for the particular circumstances.

The national security grounds in the Privacy Act need to be framed so that they complement the protections for national security information in other contexts. If it proves desirable to refine the definition of national security, consideration may need to be given to whether any revised approach should flow through to the information statutes such as the Privacy Act and the Official Information Act.

Q17 Who should decide whether national security information is disclosed to affected parties, withheld or partially released in proceedings? Should it be the courts or the Crown through the Attorney-General or the Prime Minister?

In our view, it would be more consistent with the rule of law for the courts to have this role in preference to the Executive. However the hybrid model may achieve a suitable constitutional accommodation.

Q18 Would a model under which the court determines whether the Crown's claim of public interest immunity on the grounds of national security is valid, but the Prime Minister or Attorney-General has a power to ultimately and publicly override the court's decision be workable for New Zealand?

There is a parallel in New Zealand's Official Information Act which provides a right of Executive veto of an Ombudsman's recommendation that information be released. Although it is rarely used, it provides a kind of "constitutional safety valve" and power balance between the Ombudsman as a Parliamentary Officer and the Executive.

Given this precedent, we agree that it may be worth considering a hybrid model that provides for an Executive override. As noted, this is a feature of the Canadian framework. The fact that it has never been used suggests that the provision performs a similar function in the balance of power.

It is worth noting some ancillary features of the OIA veto – it can be judicially reviewed and costs are generally borne by the Crown.[20] Theses incentives may be relevant to the design of any Executive override in the context of public interest immunity.

---

[20] Official Information Act 1982, s 32B.

Q19 Do you think there are benefits in developing an approach under which the affected person's own lawyer can represent them during closed proceedings (and not a special advocate)? How would this affect the lawyer's obligations to their client?

We support this option in preference to the use of special advocates wherever possible. Although it may create a tension for lawyers in representing their clients' interests, lawyers are professionally trained to handle competing interests (such as handling duties to the court, and duties to other members of the profession) and are subject to professional ethics.

It would be desirable for lawyers who are made subject to restrictions to be able to seek directions from the judge where necessary to guide their conduct and the conduct of the relevant proceeding.

Q20 Given the constraints under which they operate, do you think special advocates can adequately ameliorate the unfairness of proceedings when people are denied full disclosure of the case against them?

A special advocate is fundamentally handicapped in representing a party, if they are limited in communicating with them. A fundamental feature of our justice system is the opportunity to challenge the accuracy, authenticity, robustness and completeness of evidence relied on by the opposing party, and the interpretation of that evidence presented to the court. Legal counsel present argument to the Court by bringing together the full array of the facts and applying the law to them. The synthesis of facts and law is prejudiced where the lawyer/client relationship is diluted.

While special advocates could play a role in challenging the opposing case on the basis of legal argument, there are significant limitations in bifurcating representation between different lawyers.

Q21 Should we have a special advocate regime for civil and administrative proceedings? What are the key features and protections you would want to see built into a legislative special advocate regime?

Should special advocates be used in civil and administrative proceedings, safeguards should include opportunities to seek review of any procedural decisions, to verify that the departure from usual procedure is justifiable in the circumstances to protect national security information.

Q22 Do you consider that there is scope in criminal trials to use special advocates in the preliminary stages of the trial to assist in determining whether information that prejudices national security should be withheld? Do you agree special advocates should not be used in the substantive trial?

In relation to the preliminary stages, see our comments at Q2.

We agree with the Law Commission's view expressed in para 6.89 of the Issues Paper that special advocates should not be used in the substantive trial.

Q23 Do you favour a generic legislative approach that establishes one closed proceedings regime with natural justice safeguards that can be applied across all the relevant administrative and civil contexts and (possibly) aspects of criminal proceedings, or should specific regimes be retained and developed?

We support consideration of a generic legislative approach, provided, as discussed above, there is room for tailoring the process in any particular case to meet the necessities of fundamental fairness and due process.

We also think there would be benefits in adopting a flexible approach, rather than a one-size fits all, so that more open features can be used in appropriate circumstances. The least open process should be reserved for those exceptional circumstances where there is a high risk of prejudice to sensitive national security interests.

8 July 2015