Australian Government
Australian Research Council

Safeguarding National Security *and* Fairness in Non-disclosure Decisions of Sensitive Information in Australia

Submission to the Independent National Security Legislation Monitor (INSLM) September 2013

Johannes Krebs and Professor Simon Bronitt

Contact Details:

Director:	**Professor Simon Bronitt**
Telephone:	**07 3735 5938**
Facsimile:	**07 3735 1033**
Email:	**s.bronitt@griffith.edu.au**
Address:	**Australian Research Council Centre of Excellence in Policing and Security** **Level 3, Suite 3.01** **Social Sciences Building (M10)** **Mt Gravatt Campus** **Griffith University** **Messines Ridge Road** **Mt Gravatt QLD 4122, Australia**

CONTENTS

About CEPS

The Australian Research Council (ARC) Centre of Excellence in Policing and Security (CEPS) was established by the ARC in 2007 to boost policing and security research capacity in Australia in the post-9/11 environment. It is one of the largest non-science research investments in Australia based on a university partnership between Griffith University (the administering organisation), the Australian National University, University of Queensland and Charles Sturt University, as well as policing agencies including the Australian Federal Police, Queensland Police Service and Victoria Police.

Our Vision

CEPS research leadership shapes policy and practice reform to strengthen the security and well-being of Australia.

Our Goals

Research

Deliver an exceptional and internationally renowned program of research.

Education

Play a key role in developing the next generation of policing and security scholars.

Growth

Stimulate increased research and policy interest in national and international policing and security issues.

Engagement

Effectively engage the public, research, policy and practitioner environments on policing and security issues.

Distinction

Achieve national and international distinction.

The views and recommendations in this submissions are offered by the authors to assist the INSLM and to contribute to the law reform in this field. The submission should not be attributed to CEPS nodes and/or CEPS industry partners. The authors would like to acknowledge the assistance provided by CEPS colleagues, including Kate O'Donnell and Nina Westera. Errors of law, fact and judgment, remain the authors alone.

Safeguarding national security *and* fairness in non-disclosure decisions of sensitive information in Australia

Johannes Krebs and Professor Simon Bronitt[1]

Introduction

When it comes to judicial decisions not to disclose sensitive national security information, the courts have always stressed that consideration must be afforded to both national security interests and the fairness of the legal procedures.[2] These valuable interests are often difficult to reconcile and present serious challenges for the judges who are engaged in balancing two essentially incommensurable interests.[3]

The *National Security Information (Criminal and Civil Proceedings) Act 2004* (hereafter "NSI Act"), which is the subject of the Independent National Security Legislation Monitor (INSLM) review in 2013, embodies this tension. The NSI Act made a deliberate policy judgment of 'tilting-the-balance' between national security and fairness in favour of the former.[4] At the same time, the NSI Act limits non-disclosure of information (deemed likely to prejudice national security) to cases where such non-disclosure would not "seriously interfere with the administration of justice."[5]

This submission points out that these provisions have been interpreted in broadly similar ways to the balancing exercise performed under the common law, in cases where public interest immunity (PII) is claimed. It appears that notwithstanding the rhetoric emphasising the need for striking a balance and the importance of upholding the fairness of the trial process, both in the legislation and case law, security concerns appear to predominately determine the outcome of judicial non-disclosure decisions. This

---

[1] The research presented in this submission was undertaken by Johannes Krebs (ANU College of Law) as part of a doctoral program supervised by Professor Simon Bronitt, Director, CEPS (Griffith University). Johannes Krebs' PhD thesis deals with the right to a fair trial in the context of counter-terrorism in Australia and the United Kingdom.
✉ s.bronitt@griffith.edu.au and johannes.krebs@anu.edu.au.

[2] Sankey v Whitlam (1978) 142 CLR 1.

[3] "It is like asking whether one object is longer than another object is heavy.": The Honourable JJ Spiegleman, "The principle of open justice: a comparative perspective" (2006) 29 University of New South Wales Law Journal 158.

[4] See in particular Section 31, NSI Act.

[5] Section 3, NSI Act, which sets out the objective of the Act.

vulnerability equally applies to the NSI Act, which provides only limited guidance on how the various interests ought to be balanced against each other.[6]

In order for judicial practice to live up to its rhetoric and to reflect the paramount guarantee of ensuring fairness in legal proceedings, a more sophisticated approach is proposed that emphasises the importance of "checks and balances". Under this model, discussed below, the basic principles of fairness cannot be simply traded away in a balancing exercise. More clearly identifying the steps involved in the reasoning process provides increased transparency in judicial decision-making, and thus increases the legitimacy, of non-disclosure decisions made by the courts.

This submission comprises four parts. Part one identifies the issues under current NSI Act and, more generally, the doctrine of PII. Part two emphasises the political challenges that judges faces in dealing with sensitive information in legal proceedings, as well as the principles of fairness that must be considered. Part three sets out the key questions that need to be addressed when making non-disclosure decisions. Part four identifies and discusses important safeguards that should be considered in any reform of the current legislation.

This submission has been written with a focus on criminal procedures. However, the same considerations apply to civil proceedings, many of which in this field will have coercive effects impacting negatively on the rights and liberties of a person. Given of what is at stake, it is submitted that the both types of proceedings – civil and criminal - must observe equivalent standards of fairness.[7]

[6] The lack of legal guidance on how this balancing of interests should be done reflects the fact, as Vincent Luizzi points out, that "[w]e all share a common intuitive grasp of, or at least are in agreement about, what the metaphor of balancing interests entails.": Luizzi, "Balancing of interests in courts" (1980) 20 *Jurimetrics Journal* 373.
[7] *Secretary of State for the Home Department v AF* [2009] UKHL 28, at [57], per Lord Phillips.

Part One: the NSI Act and PII

The NSI Act, which was intended to augment the pre-existing PII regime, has three main objectives:

- To increase control over sensitive information before the judicial decision on disclosure;
- To allow the use of sensitive national security information in edited forms;
- To tilt or adjust the balance by giving 'greatest weight' to the Attorney General's certificate.

In relation to the first two objectives, a number of human rights issues have been identified in the literature. These identified concerns relate in particular to: delays and adjournments in mandatory closed hearings; erosion of the principle of 'open justice' and the right to choose a lawyer; the creation of prejudice and bias, as well as alterations to court dynamics and its the adversarial character.[8]

This submission concentrates on the third objective and its consequences. Much attention has been paid to the question of balancing competing interests within Section 31 orders. The NSI Act requires the judges to give the "greatest weight" to the Attorney-General's certificate. In *Lodhi* the constitutionality of the provision was challenged on the grounds that the NSI Act impacted adversely on the character of the New South Wales Supreme Court, as well as raised concerns over its compatibility with the exercise of judicial power of the Commonwealth.[9] The fact that both submissions were dismissed was presented as a vindication for the government. But it also confirmed that the judges properly retained a margin of discretion over what is 'fair' and what is not, an assessment which courts are accustomed to exercising under existing doctrines of PII.

So in effect the courts applying the NSI Act have continued to do what was common practice under PII. Analysis of common law authorities suggest that 'greatest weight'

---

[8] See for example, Anthony Whealy, "Difficulty in obtaining a fair trial in terrorism cases" (2007) 81 *Alternative Law Journal* 743; Stephen Donaghue, "Reconciling Security and the Right to a Fair Trial: The National Security Information Act" in Lynch, MacDonald and Williams (eds), *Law and Liberty in the War on Terror* (2007) 87; Phillip Boulton, "Preserving national security in the courtroom: a new battleground" in Lynch, MacDonald and Williams (eds), *Law and Liberty in the War on Terror* (2007) 96; Mark Rix, "Counter-terrorism and information: the NSI Act, fair trials, and open, accountable government" (2011) 25(2) *Continuum* 285.

[9] See *R v Lodhi* [2006] NSWSC 571, at [24]. The arguments were raised by media interests, but later confirmed on appeal in *Lodhi v R* [2007] NSWCAA 360.

invariably has been afforded to national security concerns.[10] Under the PII doctrine, as codified by the *Evidence Act 1995* (Cth), there has been clear tendency to uphold non-disclosure requests on these grounds.[11]

Arguably, therefore, not much has changed in relation to the balancing exercise, which then raises the question of whether the NSI Act was truly necessary?[12] Apart from making a strong policy and political statement, it is submitted that the NSI Act missed an opportunity to clearly define the relationship between the interests of national security and the principle of fairness. The current model maintains a 'black box' approach, which sustains a lack of transparency in decision-making, and leaves the judiciary - without meaningful guidance - to resolve the tension between competing policy interests on a case-by-case basis. As examined below, the NSI Act's permissive approach to the use of edited evidence compounds this difficulty; bearing in mind the potential for distortion and prejudice that edited evidence creates in the minds of jurors, the judicial duty to avoid unfairness in the administration of justice is seriously challenging.[13]

[10] See for example *Alister v R* (1984) 154 CLR 404, at 435, per Wilson and Dawson JJ: "Questions of national security naturally raise issues of great importance, issues which will seldom be wholly within the competence of a court to evaluate. It goes without saying in these circumstances that very considerable weight must attach to the view of what national security requires as is expressed by the responsible Minister."
[11] This point has been made in relation to PII claims in relation to police informers: see Henry Mares, "Balancing public interest and a fair trial in police informer privilege: a critical Australian perspective (2002) 6 *International Journal of Evidence and Proof* 94.
[12] Andrew Palmer, "Investigating and prosecuting terrorism: the counter-terrorism legislation and the law of evidence" (2004) 27 *University of New South Wales Law Journal* 394.
[13] See below, the discussion concerning the necessity of jury instructions.

Part Two: the politics of security versus the principles of fairness

(a) Political realities of security

When it comes to non-disclosure decisions of sensitive national security information there are a number of political realities relating to security that must be kept in mind:

First, the Executive is highly protective of sensitive national security information. This stance stems from the need to guarantee future flows of information, including from foreign intelligence agencies, that are vital to Australia's national security. The broad and sweeping nature of national security claims reflects a mosaic theory of intelligence held by many state officials, which assumes "[any] scrap of information which, in itself, might seem to have no bearing on national security may, when put together with other information, assume a vital significance."[14]

Secondly, most national security experts are located within the Executive. Assessing risk is a highly complex process, which has been developed in intelligence organisations and thus requires a specialised skill-set acquired through expert knowledge, training and experience.

Thirdly, and closely related, judges lack often lack this specialised skill-set, and are poorly equipped to make such security assessments. Judges thus naturally defer to official expert assessments of risk, displaying a reluctance to challenge the Executive's decisions in this area.[15] However, without properly assessing the relative weight of any security risk, any attempt to engage in any genuine balancing with the interest of fairness seems difficult to achieve.

It follows from these political realities that security assessments supporting non-disclosure made by experts within the Executive are rarely challenged by the Judiciary, with the attendant risk that the fairness of the legal proceedings will be adversely affected.

(b) Fundamental principles of fairness

The countervailing interest is the fundamental importance of the principles of fairness. These principles, established over many centuries, must not be abrogated by security

[14] *Church of Scientology v Woodward* (1982) 154 CLR 25 at 51.
[15] See for example *R v Lappas & Dowling* [2001] ACTSC 115 (26 November 2001), at [26]: "If that is the view taken by the appropriate government representative, I have no reason to go behind it."

claims without compelling legal and policy justification being presented to the courts. This position is based on the following arguments:

First, while judges may confront difficulties in assessing security related issues, they are in fact professionally skilled and qualified to rule on matters involving the rights and liberties of citizens. Indeed, judges have constitutional duty in a liberal democracy to protect liberties against unjustified coercive measures of the state.[16] Therefore any assessment of the impact of non-disclosure on fairness properly rests in their hands. [17]

Secondly, a trial or legal process can be either fair or unfair. An unfair trial results in a miscarriage of justice. It is for this reason that the common law and international human rights law has sought to establish a set of minimum standards essential for the fairness of the trial. In Australia, the High Court has not recognised a general right to a fair trial under the Constitution.[18] However, the High Court has long accepted as a fundamental common law doctrine, that courts have a duty to ensure that legal proceedings are fair, and that judges must devise and apply remedies to prevent abuses of process. And under the common law, the defendant cannot be subject to a trial that is unfair, and that a court must stay proceedings in cases in which permitting the trial to proceed would result in an unfair trial.[19] Thus, fairness cannot be presumptively balanced away simply because it conflicts with security interests. Andrew Ashworth has made this point in the context of Article 6 (right to a fair trial) of the *European Convention on Human Rights* (ECHR).[20] Although Article 6 ECHR is not identified as an unqualified right,[21] it is equally not qualified to the same extent as the other rights in Articles 8-11 ECHR.[22] Hence, Ashworth describes the right to a fair trial as a 'strong right'.[23] A similar approach can been found to apply to the fair trial rights under the *International Covenant on Civil and Political Rights* (ICCPR), to which Australia is a signatory. The European Court of Human Rights (ECtHR) has upheld severe limitations and qualifications to the right to a

---

[16] For the relationship between Parliament and an independent judiciary see for example Peter Bailey, *The human rights enterprise* (2009) 110; Aharon Barak, *The judge in a democracy* (2006) 56; Johan Steyn, "Dynamic interpretation amidst an orgy of statutes" (2004) 35(2) *Ottawa Law Review* 165.
[17] *A and others v Secretary of State for the Home Department* [2004] UKHL 56, at [39] per Lord Bingham, and at [178], per Lord Rodgers.
[18] *Lodhi v R* [2007] NSWCAA 360, at [74] per Spiegelman CJ.
[19] *Dietrich v The Queen* (1992) 177 CLR 292.
[20] Andrew Ashworth, *Human rights, serious crime and criminal procedure* (2002) 61.
[21] See Article 15 ECHR.
[22] Those qualified rights can be limited according to law and to the extent "necessary in a democratic society in the interests of national security".
[23] Andrew Ashworth, *Human rights, serious crime and criminal procedure* (2002) 56.

fair trial, though it has required at the same time that such constraints must be 'compensated' in the procedures.[24] The jurisprudence from the ECtHR is not always consistent in its approach, and often seeking refuge in the wording of Article 6 ECHR, rather than clarifying what constitutes a minimum standard. The question remains what constitutes this minimum threshold of fairness (and unfairness). The answer continues to be controversial.

Thirdly, under the law of evidence, there is a 'golden rule' that all evidence which is material to a case should be disclosed.[25] Any deviation from this rule carries the risk of miscarriages of justice.[26] Hence, suppression of material information should be considered the exception to this rule and thus should require clear and compelling justification. The onus of whether or not sensitive information should not be disclosed rests with the party making the claim of non-disclosure and thus generally with the Government. Although Section 130 of the *Evidence Act 1995* (Cth) is not explicit, the provision is generally understood in the same way.[27]

This is also in line with more general liberal principles that any limitation to individual liberty by the state needs to be justified and kept to its absolute minimum. Without denying or belittling current risks to national security, this area should not be excluded from this principle. This is because, as Lucia Zedner has pointed out, security is not an end in itself, but rather simply a means to create liberty.[28]

(c) Reconciling the realities of security and principles of fairness

These realities and principles have a number of consequences for any regime governing non-disclosure of sensitive information that is also committed to upholding fairness:

First, as outlined above, judges are often discomforted in being called upon to assess risks associated with the disclosure of sensitive information. At the same time they have a constitutional duty in a liberal democracy to prevent arbitrary acts of the state and uphold rights and liberties.

---

[24] In the context of non-disclosure see for example *Rowe and Davis v United Kingdom* [ECtHR] Application No. 28901/95 (16 February 2000) at 61.
[25] *R v H and C* [2004] UKHL 3 (5 February 2004), at [14].
[26] Ibid.
[27] Stephen Odgers, *Uniform Evidence Law* (2009) 655. (referring to *Sankey v Whitlam* and *Fernando v Minister for Immigration & Multicultural & Indigenous Affairs*).
[28] Lucia Zedner, "Seeking security by eroding rights: the side-stepping of due process" in Gould and Lazarus, *Security and human rights* (2007) 258.

Therefore judges find themselves in a difficult situation, particularly when legislation expressly prioritises national security over liberty. The result is what may be termed a 'legal grey hole', i.e. a situation in which the impression is generated that there is some system of judicial oversight, though in reality there is none.[29] To avoid this legal chimera of judicial oversight, legislation must refrain from directing judges in what weight to attach to particular interests. It does not follow that the proper solution is for the judges to retreat entirely from the field. Rather, security decisions that potentially impact negatively on individual liberties should be subjected to an alternative system of checks and balances. When it comes to decisions involving security assessments, judges need more (not less) assistance in fulfilling these challenging duties.

One way to furnish such assistance is through establishing a panel of Security Review Advisors (SRA) to assist judicial officers. Such a panel could be modelled on existing organisations such as the Canadian Security Intelligence Review Committee (SIRC)[30] or the British Special Immigration Appeals Commission (SIAC).[31] SRA panel members would be qualified in risk assessment by their substantial experience in the field of national security and intelligence. They would be security cleared to the necessary level and possess all the necessary knowledge for evaluating and testing the information, and to assess the weight of arguments as to why non-disclosure is necessary, including the propriety of the intelligence-gathering. Crucially, the SRA would enjoy a certain level of independence from current administration and public officials. The panel could be drawn from retired police, security and intelligence personal, and in particular from former or current Inspector-General for Intelligence and Security and staff.[32] There is also value in including in the SRA Panel specialists working outside of law enforcement/security practitioner contexts (e.g. from the corporate and university sectors). Broadening the discipline mix, for example by drawing on psychological and actuarial (statistical modelling) methods to evaluate risk, would serve to minimise distorted assessments caused by convergent thinking or 'group think' among a panel comprised of similar professional backgrounds and experience.

---

[29] See David Dyzenhaus, *The constitution of law: legality in a time of emergency* (2006) 50.
[30] http://www.sirc-csars.gc.ca/index-eng.html.
[31] http://www.justice.gov.uk/tribunals/special-immigration-appeals-commission. SIAC members are draws from different backgrounds providing different skill sets to the commission. "As specified in the 1997 Act, the SIAC panel consists of three members. One must have held high judicial office; and one must be - or have been - a senior legally-qualified member of the Asylum & Immigration Tribunal (AIT). The third member will usually be someone who has experience of national security matters."
[32] http://www.igis.gov.au/.

Given that SRA Panel will have had close connections to the Executive, and thus has some similarities to a system of internal review, such an approach may in some instances challenge traditional understandings of the separation of powers. However, the judge would still have the final say in the determination, an approach that would serve to reassure the defendant that decisions which cannot be made publicly are not arbitrary and that the claims relating to security have been subject to (some degree) of independent scrutiny. It is submitted that this model for guaranteeing both security and liberty entails strong cooperation between the branches of government, and will be guided by the values of a liberal democracy based on 'checks and balances' and the rule of law.[33]

Concern is often expressed that these additional measures would be costly. This argument should be rejected given that the legal system is dealing with proceedings involving matters of national security (including some of the most serious offences such as terrorism), some of which potentially threaten the very foundations of our society. Although there is clearly a cost burden, there is some solace that such proceedings are not (as yet) commonplace. It should also be noted that legitimacy has greatest value (even if it does impose additional cost) in cases involving the most serious of crimes. Historically, the roots of many of our common law rules designed to promote fairness in criminal proceedings were developed in relation to some of the most heinous of crimes, namely treason. Although there is an enormous public interest in convicting terrorists or persons posing a threat to the national security, it is submitted that the more serious the offence the greater attention must be paid to due process values.[34]

Secondly, any model governing non-disclosure must ensure that fairness is maximised at all times. This has the effect, in accordance with the general law of evidence, that all information that is material should be disclosed, and that any curtailment of this principle should be justified in a liberal democracy. This claim has two aspects: one aspect is that the suppression of such information should be limited only to what is 'reasonably necessary' to protect the national security interests; and the other aspect is that limitations on fairness must be 'compensated' as much as possible.

---

[33] Aharon Barak, *The judge in a democracy* (2006) 40.
[34] Andrew Ashworth, "Crime, community and creeping consequentialism" (1996) April *Criminal Law Review* 223.

It is accepted that non-disclosure of material evidence may cause a forensic disadvantage for the defendant.[35] The danger is apparent from reviewing the role that non-disclosure of material played in several notorious miscarriage of justices in the UK during the 1980s and 1990s – including the Guildford 4, the Birmingham 6, the Maguire 7,[36] and Judith Ward. The inclusion of offences criminalising unlawful disclosure seeks to address this risk: the NSI Act contains a number of criminal offences relating to unlawful disclosure of sensitive information covered by the AG's certificate.[37] As a matter of fairness, it is submitted that this criminal offence should be extended *mutatis mutandis* to cases of failing to disclose or supressing information material to a criminal trial. Admittedly such an offence would be difficult to enforce, as it would generally require an internal investigation, and there would remains some room for debate on whether evidence withheld was "material". That said, this offence would send a clear message that decisions relating to (non)disclosure in this case should be made in the courts and is not merely a matter of discretion or judgement for the Executive. Furthermore, it would impose an additional legal obligation upon the existing professional/ethical duty to disclose material evidence to the defence. Without it, there could not be an offence carrying a penalty for non-compliance.

Finally, the trial judge plays a crucial role in ensuring the fairness of the trial. Hence, it is submitted that the legislation must clearly state that the presiding judge retains control over all stages of the proceedings including decisions in relation to whether or not the court needs to be closed to the public, hearings are held *ex parte* or proceedings delayed. This avoids a number of issues that materialised under the NSI Act, and serves to increase flexibility and efficiency.[38] Above all, the judge remains in control of determining what fairness requires in any particular case with the unencumbered power to stay proceedings if necessary.

Whenever the defendant or any legal representative for the defence is excluded from the proceedings, the judge must acknowledge that the fundamental adversarial character of the proceedings has been disrupted – in other words, in these cases, the 'equality of

---

[35] See for example *R v H and C* [2004] UKHL 3 (5 February 2004), at [14].
[36] See the Interim Report on the Maguire Case: The Inquiry into the circumstances surrounding the convictions arising out of the bomb attacks in Guildford and Woolwich in 1974 available at http://www.official-documents.gov.uk/document/hc8990/hc05/0556/0556.pdf.
[37] Part 5 NSI Act.
[38] Stephen Donaghue, "Reconciling Security and the Right to a Fair Trial: The National Security Information Act" in Lynch, MacDonald and Williams (eds), *Law and Liberty in the War on Terror* (2007) 90.

arms' principle suffers a legal amputation of one of its limbs! As a consequence of the exclusion of the defendant and/or their legal representatives, and to compensate for the inequality of arms, the judge may wish to assume a more active inquisitorial role. This judicial compensation strategy does not obviate the need for a special advocates scheme. Rather it simply underscores the key role that judicial officers play in safeguarding the interests of the defendant in certain phases of the proceedings. It is also important to stress that this exclusion of the defendant and/or their legal representative should not be routinely viewed as an acceptable alternative for open trial, but rather limited to cases in which materiality of sensitive information and the extent of disclosure must be assessed.

It is likely that Australian judges would not welcome such a fundamental change to their role in court. In the common law world, inquisitorial proceedings are generally understood as non-judicial or administrative. That said, there are also a number of examples where inquisitorial models – in the continental European sense of judicial investigative role - have been adopted or suggested in common law systems. In Canada, the Supreme Court in *Charkaoui* discussed the adoption of a "pseudo-inquisitorial role" of the Federal Court in reviewing the *in camera* and *ex parte* hearings under immigration regime of the time.[39] The Court acknowledged the value of the active role of the judge in that case, rejecting claims that such an approach would endanger judicial impartiality. However, the Court expressed concerns about the accuracy of the decisions, given that the court was not provided with the full powers of an inquisitorial court or any adversarial challenge.[40] This is why the relevant procedures were held unconstitutional[41] and a regime of special advocates was introduced as a consequence. Of course it has to be kept in mind that *Charkaoui* was an immigration case and thus the court was not limited to questions of disclosure.

In Israel, the courts have adopted a "judicial management model" in administrative detention cases where only limited information is disclosed.[42] "In the framework of these proceedings the judge is required to question the validity and credibility of the administrative evidence that is brought before him and to assess its weight."[43] Moreover,

[39] *Charkaoui v Canada* [2007] 1 S.C.R. 350.
[40] *Ibid* at [50]-[51] and [63].
[41] *Ibid* at [65].
[42] For a discussion see Barak-Erez and Waxman, "Secret evidence and the due process of terrorist detentions" (2009) 48 *Columbia Journal of Transnational Law* 18.
[43] CrimA 6659/06 - *A et al. v. The State of Israel* [2008] at [43]

the judge has a duty to consider the material from the perspective of the defendant, who is excluded from the proceedings.[44]

The 'Diplock trials' introduced into Northern Ireland in the 1970s generated concern that a judge sitting without a jury would alter the adversarial character of the trial. Jackson and Doran demonstrated that judges in Diplock courts, to a certain extent, did assume more inquisitorial behaviours.[45] However, there was equally the concern that although the character of the trial did change, the role of the judge formally remained the same. Even in Australia, there are some examples where certain judicial or quasi-judicial institutions have been provided with formal or informal inquisitorial powers. However, these have been admittedly limited to certain types of Commissions, Tribunals,[46] and the Coroners Courts.[47]

[44] Ibid.
[45] This concerned the level of judicial questioning and intervention. However, they were unable to quantify the trend. Their claims were based on their empirical study into the behaviour of judges in Northern Ireland conducting ordinary trials and Diplock trials. This was possible because the two systems ran parallel – depending on the offence – and each judge in Northern Ireland had to take on some Diplock trials. Jackson and Doran, "Conventional trials in unconventional times: the Diplock Court experience", (1993) 4(3) *Criminal Law Forum* 503. See also Jackson, Doran and Seigel, "Rethinking adversariness in nonjury criminal trials" (1995) 23(1) *American Journal of Criminal Law* 1 and Jackson and Doran, *Judge without jury* (1995) Chapter 10 The Future of judging without jury.
[46] Narelle Bedford and Robin Creyke, *Inquisitorial processes in Australia's tribunals* (2006).
[47] Brian Mills, *The criminal trial* (2011) 7.

Part Three: asking appropriate questions in non-disclosure decisions

In 2004 the Australian Law Reform Commission's (ALRC) Report on sensitive information[48] suggested that in particular situations the AG's certificate should be conclusive proof of the matters therein, and it is then up to the court to decide what the consequence of non-disclosure would be.[49] Andrew Palmer has commented in this context:

> "[A]s the ALRC's proposals recognise, and as *R v Lappas* demonstrated, the question as to whether information should be disclosed, and the question as to whether – if the information is not to be disclosed – the accused can receive a fair trial, are fundamentally separate questions."[50]

Given the different nature of these questions and recognising the expertise and competence of the two branches, it is submitted that any reform of a non-disclosure regime should clearly distinguish between:

(a) *security questions*, which relate to the necessity of the non-disclosure and to what extent. Here is has to be accepted that only a very basic level of judicial scrutiny is applied; and

(b) *liberty questions*, which deal with the consequences of any non-disclosure upon the fairness of the trial. Being guided by the concept of proportionality, the aim should be to minimise the impact on the fairness of the trial by installing appropriate safeguards. At this stage, the judges are in charge and no automatic deference to security should be applied.

This view accepts that security and liberty cannot be sensibly balanced against each other without creating a 'black box' of decision-making. In its stead, this submission proposes that the NSI Act must provide for a more structured decision-making process for judges called upon to adjudicate on this particular issue. There is of course a good chance that some judges already address this issue in such a manner, and the current NSI

---

[48] Australian Law Reform Commission, Keeping secrets: The protection of classified and security sensitive information (Report 98, May 2004).
[49] *Ibid* at [11.166]-[11.167].
[50] Andrew Palmer, "Investigating and prosecuting terrorism: the counter-terrorism legislation and the law of evidence" (2004) 27 *University of New South Wales Law Journal* 394. Palmer referred to Australian Law Reform Commission, *Protecting classified and security sensitive information* (Discussion Paper 67, January 2004) and *R v Lappas & Dowling* [2001] ACTSC 115 (26 November 2001).

Act has enough scope to be interpreted in such a way.[51] However, there is an obvious benefit of a more explicit model guiding decision-making under NSI Act. This approach guarantees increased transparency, which is not only vital for reviewing decision-making processes on appeal, but also strengthens the legitimacy of the decision itself.

(a) The security question and the need to supress sensitive information

Unlike the ALRC Report, this submission does not support the view that the AG's certificate should be conclusive. In order to safeguard against arbitrary decision-making in relation to security matters, checks and balances are manifestly required. As under the current legislation, judges must review the information in question to determine whether it is withheld for legitimate reasons.[52] This is a prerequisite for any non-disclosure order. As proposed above, the judge reviewing the information should be assisted by the SRA panel. The onus rests with the party claiming non-disclosure to justify non-disclosure, which is generally the State/Executive.

The question remains what is a 'legitimate reason' for non-disclosure? It has been accepted that not only sensitive information or vulnerable witnesses deserve protection in cases where a concrete danger can be demonstrated, but protection should also extend to cases where information has been received from foreign intelligence agencies, or where information relates to the methods used by intelligence agencies. In those cases, the risk to national security may be remote or potential, but non-disclosure is regarded as vital to the continuation/sustainability of the work of Australia's security agencies. Hence, it seems that the threshold of legitimacy for withholding information is rather low.[53] Illegitimate reasons for seeking non-disclosure could apply to cases where the information is already public, the information is being withheld for political reasons, for example to avoid embarrassment, or because of bad intentions, for example to conceal serious criminality by state officials. However, even to identify those cases expertise in intelligence methods and processes is needed.

Despite the assistance of the SRA panel, it is important for the trial judge to review all relevant information it order to assess its importance to the fairness of the proceeding,

[51] Apart from the unfortunate formulations in Section 19 NSI Act, it is commonly accepted that the judge ultimately retains a power to stay the proceedings under the NSI Act.
[52] See *Alister v R* (1984) 154 CLR 404.
[53] In the UK, *R v H and C* put the threshold higher, requiring disclosure unless there is a "real risk". See *R v H and C* [2004] UKHL 3 (5 February 2004), at [36(3)].

which can also change over the course of the trial.

(b) The liberty question and determining the fairness of the trial

Considering the principles described above, determining the fairness of a trial potentially affected by non-disclosure involves two questions: the first question concerns how to safeguard the fairness of the proceedings – including *ex parte* hearings - and thus how to limit the impact of the non-disclosure. [The safeguards at the disposal and discretion of the judge will be discussed in the following part]. The second question is whether – in any given instance of non-disclosure with or without additional safeguards – the overall fairness of the trial is still guaranteed? In other words, does the non-disclosure of information require a stay of proceedings. This second aspect is not exclusively related to a non-disclosure order of a particular piece of information, but needs to be monitored continuously throughout the process.[54]

A crucial aspect is of course the importance of the information for the particular case. At one end of the spectrum is information which is not material at all. Certainly this is a question that can be addressed before addressing non-disclosure.[55] However, thematically it fits here, as there will be no issue of negative impact on fairness if the information is not properly a matter for disclosure in the first instance. At the other end of the spectrum there are cases where the information is clearly material, and indeed, crucial to casting doubt upon the guilt or innocence of the defendant. A fair trial seems difficult to imagine without such disclosure to the defendant. In such cases, the options seem limited: either the prosecution withdraws charges (enter a *nolle prosequi*) and/or the judge stays the proceedings. More difficult are cases where information is material, but it is unclear as what precisely this materiality bears upon.

Sir Richard Scott commented in this context:

> "As to documents which appear to have *the potential to assist the defence*, could a situation ever arise in which disclosure could be refused on PII grounds? This is, to my mind, a fundamental but conceptually simple, question. The answer to it, both on authority and on principle should, in my opinion, be a resounding 'No'. In the context of a criminal trial how can there be a more important public interest than that the defendant

[54] See *R v H and C* [2004] UKHL 3 (5 February 2004), at [36].
[55] This concern only cases, where the information is requested by the defense.

> should have a fair trial and that documents which might assist him to establish his innocence should not be withheld from him."[56]

Given that the NSI Act intended to permit the use of edited sensitive information, the question of whether its use contributes to or hampers fairness adds another layer of complexity. In particular it emphasises the importance of safeguards and requires constant attention by the court to the impact on the overall fairness of the trial. Unless there exist appropriate safeguards, it is submitted that criminal trials should not proceed when information that has potential to assist the defence is not disclosed. This standard should be similarly applied in civil proceedings, which as noted above, have similarly serious consequences for the liberty and property of a person. This point has been made in recent English cases involving administrative proceedings, in which the House of Lords held that the absolute minimum required to avoid 'secret justice' is providing enough information to the parties to permit them to meet the case and to instruct the special advocate retained to represent them.[57]

[56] Richard Scott, "The use of public interest immunity claims in criminal cases" (1996) 2 *Web Journal of Current Legal Issues*. (emphasis added). Sir Richard Scott was the author of *The Report of the Inquiry into the Export of Defence Equipment and Dual Use Goods to Iraq and Related Prosecutions*, 1995-96, H.C. 115, commonly referred to as the Scott Report. One of the issues of concern identified during the inquiry was the use of PII certificates.

[57] See *Secretary of State for the Home Department v AF & Another* [2009] UKHL 28 (10 June 2009). It should be pointed out that *AF* was a control order case and thus according to this submission should have deserved a higher level of due process. Furthermore, the new *Justice and Security Act 2013* (UK) does not require the defendant to be provided with a mere 'gist'. It remains to be seen whether the courts will accept this significant lowering of the standard even in civil proceedings.

Part four: safeguards to maintain equality of arms

A number of measures have been developed under the common law or by legislation in order to 'compensate' for any limitations of the fairness of the trial either during *ex parte* hearings or in cases when sensitive information is adduced in edited form. However, the effectiveness of these compensatory strategies is not always assured. In the following section, the submission examines these issues, and identifies some areas of potential reform. [Reference to 'edited evidence' in the submission includes the use of redactions and summaries, as well as anonymous witnesses; it also includes limitations of any kind to information a witness would otherwise be able to provide.]

(a) Special advocates

One of the most frequently discussed safeguards in relation to *ex parte* hearings is the role of the special advocate. The use of security-cleared lawyers – called special advocates - to represent excluded parties was first applied in Canada, and then subsequently exported to the UK. Even in Australia, Whealy J canvassed the potential use of special advocates as an option, though this was never adopted. In *Lodhi*, special advocates were viewed as a measure of last resort and ultimately were not considered necessary in that particular case. With this exception, the use of special advocates has not featured as a major point of discussion in Australia. This may be because there have only been two control order cases so far,[58] and both defendants were allowed to participate in all of their proceedings.[59] The special advocate regimes in Canada and the UK have been subject to heavy criticism by commentators, and as such adoption has not been recommended in Australia.[60]

In the UK, special advocates have been used regularly in control order cases to secure the rights of the defendant. The barristers, acting as special advocates, have highlighted numerous issues and concerns with the model applied in the UK.[61] The major issue is

[58] These are the type of proceedings where the use of special advocates has been quite prominent in the UK.
[59] In both case a lot of information had already been public.
[60] See Sue Donkin, *The Evolution of Pre-emption in Anti-Terrorism Law: A Cross-Jurisdictional Examination* (Doctor of Philosophy thesis, Griffith University, Brisbane, 2011).
[61] Constitutional Affairs Committee, *Seventh Report of Session 2004–05* (HC 323-I) Parts 4 and 5; The Committee interviewed a number of special advocates for the report; see also Martin Chamberlain M, "Special advocates and procedural fairness in closed proceedings" (2009) 28(3) *Civil Justice Quarterly* 314; and Martin Chamberlain, "Update on procedural fairness in closed proceedings" (2009) 28(4) *Civil Justice Quarterly* 448.

that special advocates, with few exceptions, are not permitted to communicate with the defendant after they have seen the classified information.

In our view, a more sophisticated and flexible regime could be devised for Australia, which provides important safeguards for defendants during *ex parte* hearings, and could even be extended to criminal trials. An Australian special advocate scheme, avoiding the pitfalls of the UK model, should have the following features:

- the provision of a special advocate should be mandatory at the request of the defence.
- a special advocate should be able to contact the defendant after the closed hearings subject to certain conditions. Although some sort of oversight could be allowed, the main responsibility should rest with the special advocate.
- a special advocate should be able to call witnesses.
- a special advocate scheme must be adequately and independently funded. In the UK special advocates have experienced difficulties with only limited access to expert assistance due to the sensitivity of the information.

(b) Edited Evidence and Jury Warnings

Whenever edited evidence is used, there is a risk that the information provided will be vague or misleading. This arises because the information is incomplete or because certain points are emphasised at the expense of others. This can be a problem for jurors in criminal trials. Of course they can conclude that the evidence is simply unconvincing and lacks credibility. However, against the background of national security concerns, jurors might be understandably tempted to interpret parts that are not disclosed in a particular way (to fill in the blanks with speculation) or to expect that there is much more material which cannot be disclosed. Hence the question remains how to value this type of evidence?

In situations where sensitive information is used in an edited form, it is submitted that the judge should give the jury a warning about these dangers. The topic was discussed on appeal in the *Lodhi* case.[62] Such warnings are optional under section 165 of the

[62] *Lodhi v R* [2006] NSWCCA 101, at [23].

Evidence Act 1995, though in our submission, these should be mandatory in these particular cases.

Another compensating strategy for edited documents is to require the prosecution together with the special advocate to write a report that would outline the extent of information that has been left out, and to identify the range of risks associated with reliance upon the edited document. The judge would overview the process to ensure fairness. This is comparable to guidelines applied by the DPP in relation to police informers whose identity cannot be disclosed. Under these guidelines, where possible, the defendant should be informed about the motivation of the informer, their state of mental health, whether or not they were paid, whether they were imprisoned at the time and any other issues in relation to their credibility, etc. This compensatory measure could also discourage the prosecution from using edited evidence unless it is clear, and thus valuable for the jury.

The use of edited evidence may also favour the interest of the defence, preventing the disclosure of material that bears negatively on the credibility of the defendant. Hence, what is required in any particular case depends on the specific use of the information, and thus the process of (non)disclosure needs to be closely monitored by to judge.

(c) Limited use of edited information

Finally, as a matter of policy, it is submitted that no conviction be solely or predominantly based on edited evidence. As pointed out above, this is due to the risks of distortion and the limitations of testing evidence in a normal adversarial fashion. This safeguard mirrors the position adopted by the ECtHR.[63]

[63] *Van Mechelen and Others v. the Netherlands*, 23 April 1997 paragraph 55, Reports 1997-III.

Conclusion

Taking security risks seriously is important, but so is preserving the fundamental principles of fairness. The former has enjoyed much attention, particularly in the post 9/11 era, which is why regular reminders not to neglect the latter are necessary.

It has to be accepted that in particular circumstances non-disclosure of sensitive information and/or the use of it in edited forms will render a trial unfair. Legislation expressing an equal commitment to fairness must separate the question of security from the question of fairness. Once sensitive information is used, including anonymous witnesses or edited evidence, enhanced safeguards should be at the disposal of the judges to ensure that equality of arms is maintained, and the fairness is not crudely traded for security.

The true challenge in this process remains with the judges in determining what precisely constitutes a fair trial. It is assumed in this submission that all branches of government share an interest in protecting liberties and security. Hence, Parliament should create a legislative regime supporting the judges in this difficult task, rather than shifting the responsibility exclusively to the courts and expecting the judges “to do the right thing”.

Finally, a successful approach can only be realised once other related areas are equally addressed and reformed. This concerns, for example, the rules and regulations to avoid the tendency towards over-classification of information. In particular, procedures must be put in place to increase the possibility of disclosing of information that stems from foreign intelligence organisation and is classified only because of that fact. Furthermore, intelligence organisations have to become more aware that such information may be used in court and adjust their processes and rules of engagement with foreign intelligence agencies accordingly.